Issue #121
29 September 2016

Attempted theft of $500,000 via cyber-attack on real estate agency

A Perth real estate agent is breathing a sigh of relief after a cyber-attack was thwarted in an attempt to steal $500,000 from a trust account.

It's believed the cyber thieves gained access to the agency's bank accounts after malware was downloaded into their computer system, probably from an attachment being opened or a website link being clicked in a scam email. The installed malware allows the criminals to record keystrokes and discover bank log in details, including the password.

The unauthorised withdrawal of $500,000 was discovered by a staff member the next morning who immediately contacted their bank. The bank commenced action to have the transfer terminated and the funds returned. The money had not been collected by the scammers so the transaction was stopped and the funds were successfully recovered.

Acting Commissioner for Consumer Protection David Hillyard praised the quick action of the staff member who had prevented a devastating loss.

"A delay in reporting this loss and requesting stops be placed on the transfer could have resulted in the funds being in the hands of scammers and the agency facing a financial disaster," Mr Hillyard said.

"We commend the quick action that was taken which robbed the scammers of a huge windfall from their criminal activities and maintained the agency's financial integrity. The agency's best practice standard of reconciling their trust accounts daily was integral to their picking up on the theft quickly.

"Even though the theft was prevented, the agency has implemented new and more secure connections to its bank through the use of a real-time device commonly called a Security Token which changes the internet banking authorisation passcode on a continual basis.

"Two people are now required to independently enter their system-generated and unique passcode to jointly authorise all transfers of funds out of the trust account. These measures ensure that an unauthorised transfer request is rejected and the agency is advised."

In February 2014, a Broome real estate agency lost $50,000 after scammers accessed the agency's online banking system and changed the bank account details of their clients who were on a 'pre-entered list' of recipients for regular payments. The account details were later changed back to the original in the hope that the fraud would not be detected. The agency was reimbursed by their bank.

In March 2013 a Perth settlement agency had $50,000 in two BPay transactions taken from their trust account but the suspicious transactions were detected early by the bank and the money was recovered.

Mr Hillyard said people, not only working in real estate but in all businesses, need to be careful about the attachments they open or the links they click on contained in seemingly innocuous emails.

"Giving cyber criminals access to your computer by unknowingly downloading malware means the thieves can compromise your accounting and banking system or they can even

spoof emails of executives, tricking staff in to making payments. Staff should be trained to recognise the risks and query these emails to prevent incursions.

“Every business should have procedures and protocols which will prevent unauthorised access to their computer system and to detect malware. Having up-to-date anti-virus and anti-malware software is essential.

“Regular checking of bank account balances and daily reconciling of accounts may uncover unauthorised withdrawals in time for them to be stopped. We advise staff working in the finance area have strict processes around money transfers and changing supplier bank account or contact details.

“Businesses should discuss their online banking security measures with their bank who may recommend extra measures to provide some peace of mind.

“In this latest instance, the agency had put in place all reasonable securities and processes however the scammers were still able to trick the system into commencing the transaction to fraudulently move $500,000 out of their trust account.

“Only through the quick actions of a very diligent staff member had the crime been foiled on this occasion but everyone needs to be vigilant so they don’t fall victim to these cyber criminals.”

Organisations targeted by cyber-attacks and scams can report the details to WA ScamNet at Consumer Protection by calling **1300 30 40 54** or by emailing consumer@commerce.wa.gov.au.

Some tips that may prevent fraud losses:

- Ensure they have the latest security software (e.g. anti-virus, anti-spyware, firewall) installed on their computer systems and keep their operating system up-to-date.
- Remind staff of basic electronic security measures. If suspicious emails from any source contain an attachment, do not open them as they may contain malicious software (i.e. malware). Delete these emails immediately. Do not click on any links within these emails.
- Consider using security tokens for e-banking and ensure the device protocols are set to the highest possible level for all staff members.
- Do not store payee lists within your online bank accounts as there are many ways to manipulate these entries. When creating an electronic transfer of funds, the payee’s details should be entered manually on each occasion.
- Be wary of unsolicited emails purporting to be from your bank as some of these may be spam or hoaxes.
- Be aware that banks will never ask you to supply any of your details via email.
- When accessing your bank online, always type the address into the address bar. Never click on an online link or ‘favourite link’ to access your bank’s webpage as these can be manipulated to send you to a counterfeit site (known as phishing). While these sites may look very similar to your banks website, they are operated by fraudsters to obtain your personal banking details and passwords.