Government of Western Australia
Department of Commerce

Settlement Industry e-Bulletin

An electronic bulletin from the Consumer Protection Division of the Department of Commerce

Issue 23

20 March 2013

Weblinks

CPD Information

Newsletter Archive

e-Bulletin Archive

Departmental Publications

Contact Us

Privacy Statement

Copyright

Another attempted cyber fraud

A Perth settlement agency has been the target of another attempted cyber fraud. Fraudsters successfully infiltrated the agency's banking system and authorised two BPAY transactions which were $25,000 from a General Account and $25,000 from a Trust Account.

Fortunately, this particular fraud was caught in time and the money recovered, but it is a timely reminder of the need to have appropriate and up-to-date security software on all agency computer systems.

Background

Two weeks prior to the fraud, the agency's IT technician discovered password hacking malware on the server. It appears the malicious software was hidden within an attachment sent as part of a spam/hoax email.

While the technician managed to clear the system, the fraudsters had already set up a 'travel account' on a staff member's online banking BPAY payee list.

The fraudsters sat dormant for two weeks and then struck.

While the agency uses banking Security Tokens, it appears as if the staff member whose BPAY payee list was compromised had a different access protocol.

A Security Token is a small electronic device which provides a second level of authentication for an e-banking service when used in conjunction with an Access Number and PIN.

At the push of a button, a Security Token generates a once-only number which must be entered to continue a banking session. The numbers change frequently (for the bank in question it is every 36 seconds) and each number can only be used once.

In this instance, the staff member with the compromised payee list was only required to enter a Security Token identification number when transferring funds and not upon logging into the e-banking account.

The bank has since changed the protocol and this now means all agency staff members must use Security Token identification when logging in and again for any funds transfer request.

Importantly, while the agency had $10,000 daily withdrawal limits set up on their accounts, the bank they deal with has an extraordinarily high limit set for BPAY transactions. That is, BPAY transactions were not included in the agency's daily limits.

Most banks operating in Australia have limits on BPAY transactions, although these vary considerably. In some cases, customers can choose personal limits for BPAY transactions and/or set daily limits on the total of all banking transactions (which include BPAY).

...continued on page 2

Government of Western Australia
Department of Commerce

Settlement Industry e-Bulletin

An electronic bulletin from the Consumer Protection Division of the Department of Commerce

...continued from page one

In this instance, the bank's fraud department noticed the unusual withdrawals and contacted the agency. As such, the transactions were halted before the fraudsters had access to the money. Despite being thwarted, the agency's IT technician believes the fraudsters are still trying to infiltrate the agency's computer servers.

The licensed director of the agency believes they were lucky not to have their accounts totally cleared out. They have since deleted all entries stored in their BPAY payees list and now enter the names manually each time.

Key Points

It is clear agencies will continue to be targeted by fraudsters, so the Department recommends agents:

- Ensure they have the latest security software (eg anti-virus, anti-spyware, firewall) installed on their computer systems and keep their operating system (eg Windows 7) up-to-date.
- Remind staff of basic electronic security measures. If suspicious emails contain an attachment, do not open them as they may contain malicious software (ie malware). Delete these emails immediately. Do not click on any links within these emails.
- Consider purchasing security tokens when using e-banking and ensure the device protocols are set to 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.

The Department's Scamnet website contains a range of valuable information relating to business and consumer fraud. If you believe you have been a scam/fraud victim, you can talk to WA ScamNet about it by calling 1300 30 40 54 or emailing wascamnet@commerce.wa.gov.au.

The WA Police website has a dedicated scams/fraud section.

Scam attempts should be reported to the Department on 1300 30 40 54 or consumer@commerce.wa.gov.au or WA Police on 131444. Providing a timely account of fraud attempts enables the Department to warn the industry of potential scams and helps prevent further losses.

More information

Phone porting scam
Real estate scam 1
Real estate scam 2