15 March 2013

Protect your business from cyb crime

Uncategorized

By Talking Shop Share

Sophisticated criminal gangs are putting Australian businesses at risk by attempting to take over their computers, stealing security information such as passwords and using these to siphon money from their bank accounts.

Although they may be situated thousands of kilometres from Australia, the gangs gain access to computers or information through infected websites (which can track what you do or look at what you type on your computer) and through 'phishing' emails – these are legitimate-looking emails that aim to trick people into clicking on links and entering private information, such as personal information, passwords, pins and access details.

Once they have your information, criminals can gain access to secure banking systems or even remotely use your own email system to send different payment instructions to debtors and other business partners. Ultimately, their aim is to transfer money out of businesses' accounts by working from the inside with your security and personal information.

What you can do

Businesses can help protect themselves from cyber crime with a few simple steps:

1. Guard your information:

Business account details should never be written down and only authorised personnel should be given access to conduct transactions. Details pertaining to your personal accounts should not be shared with anyone. The best security is NAB systems in partnership with personal vigilance.

2. Up to date systems:

Make sure computers have anti-virus software that regularly updates and that they're regularly patched with software updates.

3. Think before you click:

Criminals send well-crafted, legitimate-looking emails purporting to be from legitimate entities such as banks, customs, police, tax office etc. They try to trick businesses into clicking on Internet links that download malware onto their computers. If an email seems suspicious or out of the ordinary, think before you click and check with the person who is supposed to have sent it by calling them on a phone number that you find independently – not one that is included on the website or in the email.

4. Dual authorisation:

Configure your NAB Connect business Internet banking account to require two people in the business to authorise transactions, making fraudulent activity more difficult.

Show me research and insights for:

Filter by Category:

Business topics
Economic commentary
Industry insights
Publications

Filter by Tags:

Cash flow Economy Exporting Management Property Tax Videos Wealth All tags

Search

Subscribe to Business Research and Insights

Views

Business View
Agribusiness View
Health View

Subscribe to receive View updates

Let a business banker contact you. Request a call back

Find a Business Banker near you

Visit NAB Business banking website

Try our product selector tool

Archive

What NAB is doing to protect your business

NAB has significant resources dedicated to fraud prevention and cyber security, with a team of over 100 people working 24 hours a day against fraudsters and online attacks. The team conducts around the clock 'sweeps' of the Internet looking for phishing sites made to look like NAB sites and stolen banking details or passwords. "We want to make sure our business customers can conduct their business securely and ensure their banking experience is always safe, easy and reliable," says Nick Scott, Head of Cyber Security at NAB.

NAB's cyber security team not only monitor the local online environment to guard the bank, the group of highly trained experts constantly scour the web for future threats and suspicious activity. "While we have teams of specialists constantly watching and assessing, it's important our customers are vigilant in protecting their privacy and security information such as passwords and PINs, and are alert to suspicious emails or downloads while online."

Fraud detection

Working closely with the Cyber Security team is the NAB Financial Crime team who monitor business account activity to detect irregular account transfers and spending on credit cards. When a transaction occurs outside the normal behaviour of the account holder, such as payment to another country, an alert is sent to a Financial Crime team member, who assesses the transaction and contacts the customer for confirmation.

The account is temporarily blocked and monitored until the transaction is confirmed fraudulent or deemed valid. The NAB Financial Crime team also examines the 'electronic signature' of bank account logins to look for indications the customer's machine has been taken over or is infected with malicious software (malware) designed to gain unauthorised access to computer systems.

To further protect businesses against cyber fraud, online payments trigger a text message to a customer's mobile phone asking them to confirm or block the transaction. In order to receive these added security features it's important to register via NAB Online Banking as it makes it more difficult for criminals to steal from customers' accounts, even if passwords have been stolen.

NAB's point of sale devices such as EFTPOS machines, are tamper-evident making it very difficult for criminals to install 'skimmers' – illegal devices used to steal credit card information for fraud.

Protect your business

For more information about how NAB can help protect your business from cyber fraud, contact your NAB business banking representative or the business banking call centre on **13 10 12**.

This article was first published in *Talking Shop*.

Read more Talking Shop articles (PDF 1,175 KB) articles.

Tags: **Cash flow**, **Merchants**, **Retail**, **Small business**, **Talking Shop**, **Technology**

Like 0 Tweet 0 +1 0 Share 6

July 2013
June 2013
May 2013
April 2013
March 2013
February 2013

> Show More

About the Author: Talking Shop

Talking Shop:

talking shop

Talking Shop is published by NAB's Merchant Solutions team to provide our merchant customers with relevant industry updates and insights to help manage their business more effectively. Contact us at **merchant_news@nab.com.au**

> Read Talking Shop's profile

Most recent article by Talking Shop:

15 January 2013
Talking Shop – Summer 2012

2 Other Articles

Related Articles

30 September 2010
Free up cash in your agribusiness

28 April 2011
Turning debtor invoices into cash

02 November 2012
Tips to getting paid on time

NAB Blogs | **Business Research & Insights** | **Help & guidance**