ausBIZ

October 2018

THE BUSINESS NEWSLETTER FROM AUSWILD & CO
PO Box 527 Kogarah NSW 1485
Chartered Accountants and Business Consultants

Website: www.auswild.com.au
Telephone: (02) 9588 0100
Facsimile: (02) 9588 7865

BEWARE OF THE INVOICE SCAM

A recent report that four businesses in WA including a Perth car dealership had suffered a $85,000 hit after being caught by invoice payment stings, serves as a timely reminder to all businesses of the need to be alert to this type of fraud.

WA's Commissioner for Consumer Protection, David Hillyard, said that businesses frequently transferring large sums of money, such as car dealers and other businesses selling high-value items as well as real estate agencies, are a particularly strong target for scammers.

According to Mr Hillyard's office, the unnamed dealership received an invoice with correct details following a purchase from a supplier. But the trouble came a week later when the business received an email directing the invoice be paid into a new bank account.

In an attempt to validate the request, the car dealership asked that the request to incorporate the new bank details be made on company letterhead, which was subsequently done.

Verbal confirmation was also sought, and although the listed contact number on the letterhead went unanswered, the invoice was subsequently paid.

It was only when the legitimate supplier later contacted the dealership to chase the outstanding bill that the scam was detected.

"All businesses need to be alert to attempts by scammers to intercept payments that flow to and from their accounts and ensure their email accounts and computer systems have security software to reduce the likelihood of becoming a victim of hacking," Mr Hillyard said.

The important safeguard is to establish anti-fraud measures that independently double check if a regular supplier provides different bank account details for the payment of invoices.

Closely scrutinise all invoices and query any changes to ensure that the payments are going to the correct accounts. Get a verbal confirmation of email requests to change the bank account details of suppliers and clients and ensure all staff members are aware of the anti-fraud procedures and the importance of adhering to them without exception.

"Sending a confirmation of any changes to the supplier's original email address on file, or calling them on known phone numbers, can alert them that fraudsters may be trying to intercept the payments. Don't rely on contact information contained in the suspect invoice as these may also be fake."

"Accounts staff should consider having a list of designated single points of contact with businesses to whom they make regular payments, so changes can be verified easily and quickly, and any fraud attempts can be detected before payments are made."

Mr Hillyard added: "Sometimes the accounts staff will get a fake email purporting to be from the business manager requesting an urgent payment be made to a particular bank account belonging to the scammers. If a request seems unusual or strange, query it and confirm it before paying."

This loss comes amid a series of warnings from the ACCC about fake invoices and overdue payment notices circulating nationwide.

Scammers commonly use well-known brand names like Telstra, Optus, Microsoft and even government agencies like NBN and the myGov portal to lend credence to their malicious emails.

This practice known in the cybersecurity industry as "brandjacking" takes many forms. In another variation, the scammers exploited MYOB's brand name to persuade potential victims their email message is a legitimate invoice notification.

The message from MYOB looks like a very straightforward and legitimate invoice notification. It urges the recipient to "view invoice," but is just a scam to get the victim to click on a malicious link which can deliver malware like viruses or trick their victims into giving their login credentials or credit card information to phishing sites.

Brandjacking is a growing problem and a very useful tool for scammers because they leverage the trust people place in big companies to deceive them. Cybercriminals know people can be tricked – after all, people are not machines; we're all capable of having a momentary lapse of judgement and/or making bad judgement calls – and that's why they send out millions of scam messages and put so much effort into making them look convincing.

*aus*NEWS! *aus*NEWS! *aus*NEWS!

*Our **CONDOLENCES** go to* **Vicki Trotter** *and family on the sudden passing of* **Lindsay***……and to* **Greg Jepsen** *and family on the passing of his father,* **Cec***……and to* **Joe & Diane Rinaldi** *and family on the passing of Joe's father……birthday greetings this month go to* **Natasha Finlay***,* **Stacy Thornton***,* **Luke Culbert** *and* **Sylvia Zammit** *all of whom celebrate special birthdays this month. **HAPPY BIRTHDAY** to you all……and **CONGRATULATIONS** to* **John & Trish Muir** *who recently celebrated their 50th Wedding Anniversary!*