# ausBIZ

**MAY 2017**

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

## PROTECTING YOURSELF FROM SCAM EMAILS

The more you use the internet, the more you appreciate its convenience and access to services such as banking, online shopping or paying bills. Unfortunately, the internet today is also increasingly being exploited by crooks out to scam the poor unsuspecting user.

You get an email, text message or phone call out of the blue from someone saying they are from your bank. They say there is a problem with your account and ask you to give them your account details or click on a link. If you give them these details, the scammer can use the information to steal money from your bank account. This is what is known as a phishing scam.

Phishing emails, text messages or phone calls come from scammers pretending to be a bank, financial institution, phone company, an energy company or even the Australian Taxation Office.

If it is an email that you receive, everything on the email will look like the 'real thing', from the web address to the logo and message format. However, the links provided will be to a fake website scammers have created. The website will even have a similar web address to the bank's real website. The scammer wants you to give them your personal details, bank account numbers, credit card numbers and most importantly, your passwords.

The email may ask you to download their security software which is really a trojan virus. The virus could infect your computer and give someone else control of it. It could also track your key strokes to get your user names and passwords.

According to the Australian Securities and Investment Commission (ASIC), some of the biggest names on the internet have already been targeted –

- **Commonwealth Bank of Australia, ANZ Bank** – customers were sent e-mails advising them to log their account details to re-activate their account following the introduction of a new security system. Although the URL displayed was similar to the CBA/ANZ address, it in fact directed users to a non-CBA/ANZ site.
- **eBay** – this involved a series of fake e-mails used to steal users' credit card numbers and to commandeer eBay customers' accounts and then defraud buyers using the eBay service.
- **Australian Taxation Office** – deceptive e-mails stating that you are due to receive a tax refund.
- **Origin Energy** – customers were advised of an outstanding bill and to contact a 1300 number or go online if anything was unclear. The footnote was a reminder to pay the bill by its due date, or you may have to pay a $12.00 late payment fee.

So, what are the warning signs? According to ASIC, the email or text message you receive is definitely a phishing scam if it:

- Claims to be from a bank or company that you do not have an account with
- Contains a link that leads you to a website where you are asked to enter your bank account details
- Says your details are required for security and maintenance upgrades or to 'verify' your account

- Says you are due to receive a refund for a fee that you were mistakenly charged
- Says you are due to receive a tax refund even if you use an accountant or tax agent for lodging your income tax return
- Does not address you by your full name
- Does not have your address or account/customer number
- Has spelling errors or grammatical mistakes
- Is a survey that offers you a reward or prize for filling it

How can you avoid being conned by phishing scams? ASIC says that using the internet for banking, paying bills and shopping online is safe as long as you follow these simple rules:

1 When accessing websites, don't use the links provided in emails or texts – type the address into your browser and check the website address carefully to make sure it is correct.

2 Only use your PIN through the official login site offered by your provider. Keep those sites in your 'favourites' folder and log in that way to cut down the risk of mistakes or deception.

3 Check official websites for announcements. No reputable online service provider would ask for your private account or credit card details by e-mail. If in doubt, contact the business through its official site or phone.

4 Use only secure sites for keying in financial or personal information. Look for a padlock icon at the bottom of your web browser (although some of the more sophisticated scams use 'secure sites' showing a padlock to give users a false sense of security!).

5 For Australian sites, look for the '.au' domain such as '.com.au' or '.net.au'. Anyone registering a '.au' domain must show a link between the proposed URL and an Australian trading entity. So far, ASIC has not come across a phoney '.au' site, although that does not guarantee it will never happen.

6 Avoid conducting personal or banking transactions at internet cafes, community centres and libraries. There is always a possibility that software has been loaded on by criminals that records your keystrokes. Also make sure that no one is looking over your shoulder and keep private information out of chat rooms and e-mails.

7 Don't open any email that you think could be from a scammer – delete it.

8 Don't click on any links in a suspicious email or open any files attached to it.

9 Don't call a phone number that you see in a spam email or text message

10 Act quickly if you think you have been conned. Contact your bank, credit card company or service provider immediately. This helps to protect you.

With one in twenty Australians falling victim to various scams or personal fraud every year, we should all be vigilant about phishing scams.

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

***Happy Birthday*** *to* **Tony Azzi** *who celebrates a special birthday this month.....and* ***Congratulations*** *to* **Sean Sloane** *whose over 45's hockey team won a bronze medal in the recent 2017 World Masters Games held in Auckland.*