Six scams to watch out for in 2016

Ryan Boutland – from Your Life Choices

Start the New Year on the right foot by getting a step ahead of the scammers. Keeping an eye out for these latest scams will help you to keep your money and personal details safe.

Fake parcel delivery notifications

One of the biggest scams of 2015 was the fake parcel delivery notification, which delivered malware in the disguise of an Auspost tracking notification. With online shopping growing more popular every year, this scam is probably not going to be going anywhere anytime soon. Always be vigilant if you receive an email from Australia Post and if you're in doubt simply call or visit your local post office, where someone can verify the report. Or you can check up on Australia Post's scam alerts page.

Macs being targeted

Macs are becoming more popular, and if you use an Apple computer and don't have virus protection, you might want to consider getting some as 2015 saw Mac computers receive more malware attacks than in the last five years combined.

Phone and ISP scams

Whether it's a call or an email from your phone or internet provider, if it seems suspicious, hang up/close the email straight away. Now look up the phone number for your provider on either Google or in a phone book; never click the link to its website in the email, or call the number listed as it's probably fraudulent.

Now you can call your ISP or phone provider and explain the situation. If you do this, the worst-case scenario is that you hang up on a genuine Optus or Telstra technical support employee, which is nothing compared to the hassle of a computer hack or stolen credit card details.

Social network sellers

Selling items over Facebook or other social networks is becoming more common, probably due to the friendly nature of the transactions. However, like all good things, this easy going process is often taken advantage of by unscrupulous people who may request payment in advance, and then disappear from the social network. If you don't feel confident with the transaction (for example if their Facebook account doesn't look legitimate), simply don't take the risk, stick to websites with buyer protection, such as ebay.

Emails pretending to be from your bank

A scam that sadly never goes out of fashion: the fake bank email. As with the phone and ISP scams above, make sure you proceed with caution and never follow links or call the phone numbers listed directly in the email. Also, be on the lookout for website domains which are a little off. For example, Australian websites almost always end in '.com.au', so if you're given a link heading to www.nab.com, rather than www.nab.com.au, you should close the email and contact your bank either in person, or via a phone number you know is genuine.

PayPal gifts

On the topic of suspicious internet sales, when dealing with a stranger on PayPal you should never send a payment marked as a gift. Scammers often say to send the money as a gift because you don't have to pay as much in transaction fees, which is true. But the reason you don't have to pay any fees is because there is absolutely no buyer protection for money sent as a gift.

Scamwatch is a great website for staying in the know when it comes to scams.

Be vigilant – Don't get caught