



16 February 2018

Hi everyone

Just an update:

Except for the unfortunate break and enter in Banzai Street in January (mentioned in last month's email) I haven't heard of or seen any local criminal activity (apart from stolen bikes around Casuarina and Cabarita). Always a good idea to keep our garage door closed and front door and gates locked.

I have just seen that there will be an announcement next Monday at 10.30am from Geoff Provest - State Member for Tweed regarding bike track lighting and refurbishment. (He will be at Casuarina beach entry 11 on the bike track at Casuarina Central Park). The main park is at the T intersection of Casuarina Way and Barclay Drive.

### **'Useful Telephone Numbers':**

Tweed Heads Police Station: 07 5506 9499

Emergency: Fire, Ambulance, Police: 000

Police Assistance Line: (non emergencies only) 131 444

Crime Stoppers: 1800 333 000

SES: 132 500

Power Outages: 132 080

(Unfortunately it seems that the 'After Hours Doctor' service is currently not servicing our area i.e. Salt or Casuarina).

Drop me an email if you have anything to report or would like passed on to our neighbours. Thanks.

Regards, Linda.

## **Please find below another reminder from 'Scamwatch' covering recent phone scams.**

'Why you should never trust a call from an unknown number and other tips for identifying scams.'

Have you been getting missed calls from overseas numbers or people pretending to be from Centrelink or the Australian Taxation Office?

These are just some examples of common phone scams that have occurred over the past few months, which have conned many Aussies into parting with their hard-earned cash.

Here's what you should do if you think a phone call sounds like a scam.

Almost 40 per cent of scams in Australia committed over the phone

Yep, according to Scamwatch, phone calls are the most popular for scammers in Australia.

That's followed by email at 26.5 per cent and text messaging at 15 per cent.

"[Phone calls are] so easy, it's very cheap and in countries where labour is cheaper, you've got whole call centres devoted to doing these sort of scam calls and I think that personal touch gives them a greater likelihood of getting more victims," Australian Competition and Consumer Commission (ACCC) deputy chairwoman Delia Rickard said.

Anyone can be targeted

Scammers target indiscriminately — no matter your age, income level or background.

Lately, an international scam dubbed "wangiri fraud," roughly translated to mean one ring, has seen scammers use phone numbers, possibly bought legally or on the dark web, to dial phone users in other countries. They usually disconnect the call after a few rings, hoping you will call them back.

ACCC's Scamwatch said they had 277 reports last week about the scam — which was a 794 per cent increase.

But it's not the only one. Scamwatch also said they had received complaints about scammers pretending to be from Centrelink or the ATO.

In August, scammers impersonating National Broadband Network (NBN) staff were cold-calling unsuspecting consumers and conning them into handing over sensitive personal identification details.

So, how can you tell if a phone call might be a scam?

Ms Rickard says there are a few ways you can tell you might be on the phone with a scammer, including:

If they claim to be from a computer software company wanting access to your computer. "Microsoft, Telstra, etc are not remotely checking your computers unless you have been in contact."

If the overall quality of the call is poor

Calls made on behalf of government agencies asking for bills to be paid in the form of pre-paid gift cards — such as iTunes

If the caller is applying inappropriate pressure — including threats and potentially inappropriate language, as part of their scam

Any calls asking for financial details (such as credit card or banking details)

Telstra has also warned its customers on its website to avoid callers that claim to be from the Australian Federal Police, wanting you to help them "track down criminals".

"In these calls you're often asked to transfer money abroad using international wire transfer services," the telco said.

What should you do?

It might seem obvious, but Ms Rickard says the best thing you can do to protect yourself during a dodgy call is **HANG UP**.

Otherwise, the ACCC recommends the following options:

Don't respond to numbers supplied in an automated call or from numbers you don't recognise

Always be sceptical and if you're unsure the person on the end of the phone is not who they say they are, hang up and call the organisation directly on an independently verified number

Don't give someone who calls you out of the blue any money, personal details or access to your computer

Don't return calls to international numbers unless you know them

Don't pay with an iTunes gift card. No legitimate business in Australia is going to be asked to be paid this way

Delete any messages left on your voicemail

Speak to someone you trust about the scam call

If you do think you've been scammed, it's unlikely you'll get your money back.

However, there are some ways you can limit your losses — including contacting your financial institutions, reporting the scam to authorities, changing your computer password or attempting to recover your stolen identity.

How does the scam work?

The scammers are quite sophisticated in the techniques they use to con people out of money, often pretending to be from an organisation that intimidates people.

"Talking to people who have been scammed, people are very nervous of Centrelink, they're terrified of any impact on their pension or whatever it is and they tend to do unquestioningly what they are told," Ms Rickard said.

In some cases, the scammer will try to convince someone they've done something wrong, and then demand payment as part of a solution to the problem.

But in the case of the wangiri scam, the scammers make money by using companies that sell premium numbers, allowing purchasers to work out how much they want to charge people calling them back.

That means callers who ring the international number back will be calling a premium service — meaning the telephone provider will be charged at a normal rate as well as whatever the scammer determines that call is worth — with some of the money also going to the premium number provider.

In this case, the wangiri scammers want the caller to stay on the line as long as possible, thereby increasing the amount of money they make.

If people I know have been targeted, does that mean I'm next?

Not necessarily, some of it is a result of scammers using an automated system, which allows them to call random phone number combinations.

"But, it could come through multiple ways," she says.

"We know on the dark web all sorts of lists are sold, including people who have never shown any interest in scams and so are more susceptible to these things," Ms Rickard said.

"When you go online and put your name in competitions, surveys that are doing the rounds on social media, sometimes they are put up by people who sell this information onto scammers."

People can report scams and get information at [www.scamwatch.gov.au](http://www.scamwatch.gov.au)

