Scamwatch radar alert

Monthly average losses to NBN scams almost triple in 2019

Dear radar subscriber,

Australians are losing more money to NBN scams, with reported losses in 2019 already higher than the total of last year's losses.

Consumers lost an average of more than $110,000 each month between January and May this year, compared with around $38,500 in monthly average losses throughout 2018 – an increase of nearly 300 per cent.

"People aged over 65 are particularly vulnerable, making the most reports and losing more than $330,000 this year. That's more than 60 per cent of the current losses," ACCC Acting Chair Delia Rickard said.

"Scammers are increasingly using trusted brands like 'NBN' to trick unsuspecting consumers into parting with their money or personal information."

Common types of NBN scams include:

- Someone pretending to be from NBN Co or an internet provider calls a victim and claims there is a problem with their phone or internet connection, which requires remote access to fix. The scammer can then install malware or steal valuable personal information, including banking details.
- Scammers pretending to be the NBN attempting to sell NBN services, often at a discount, or equipment to you over the phone.
- Scammers may also call or visit people at their homes to sign them up to the NBN, get them a better deal or test the speed of their connection. They may ask people to provide personal details such as their name, address, date of birth, and Medicare

number or ask for payment through gift cards.

- Scammers calling you during a blackout offering you the ability to stay connected during a blackout for an extra fee.

It is important to remember NBN Co is a wholesale-only company and does not sell services directly to consumers.

“We will never make unsolicited calls or door knock to sell broadband services to the public. People need to contact their preferred phone and internet service provider to make the switch,” NBN Co Chief Security Officer Darren Kane said.

“We will never request remote access to a resident’s computer and we will never make unsolicited requests for payment or financial information.”

“If someone claiming to work ‘for the NBN’ tries to sell you an internet or phone service and you are unsure, ask for their details, hang up, and call your service provider to check if they’re legitimate. Do a Google search or check the phone book to get your service provider’s number, don’t use contact details provided by the sales person,” Ms Rickard said.

“Never give an unsolicited caller remote access to your computer, and never give out your personal, credit card or online account details to anyone you don’t know – in person or over the phone – unless you made the contact.”

“It’s also important to know that NBN does not make automated calls to tell you that you will be disconnected. If you get a call like this just hang up.”

“If you think a scammer has gained access to your personal information, such as bank account details, contact your financial institution immediately.”

More information about NBN scams is available online at: nbnco.com.au/scamadvice.