



# Media release

Embargoed until 7am Monday 17 August 2020

## NBN Co launches community education campaign during National Scams Awareness Week

- **nbn** themed scams are one of most common scams reported to Scamwatch, with more than 2,300 reported between January and June this year with losses of \$320,624.
- Australians lost more than \$900,000 from NBN impersonation scams in 2019 with the highest number of reports and losses coming from people aged 65 years and older
- NBN Co has partnered with Scamwatch to raise awareness on the evolving nature of scams and tips for how the community can stay safe, with free information sessions to be held nationally.

NBN Co is continuing to grow its efforts to educate the community with scammers increasing their focus to deceive Australians, with new and variations of common **nbn** themed scams emerging in recent months.

As part of National Scams Awareness Week, **NBN** Co will host information sessions across the country and will leverage the latest insights and intelligence from Scamwatch in order to raise awareness about the most common and emerging scam trends and share tips about how to stay safe.

The ACCC's 'Targeting Scams' report noted that **nbn** themed scams were the most commonly reported scam type via the Australian Communications and Media Authority, with the 'Nicole from **nbn**' robocall scam the most prolific example.

Recent reports to **nbn** and to Scamwatch indicate 'Nicole' has been joined by 'Carol' in addition to the emergence of two new **nbn** themed scams including:

- residents being sent a fraudulent **nbn** invoice for payment after they were offered a **nbn** upgrade over the phone; and
- scammers claiming radiation or harmful UV rays will come from the computer and instructs the individual to move away from or cover the screen, allowing the scammer unmonitored remote access to the device.

It is important to note that NBN Co does not issue invoices direct to customers unless work has been agreed to by **nbn** and the customer.

**NBN Co's Chief Security Officer, Darren Kane**, said that ongoing education and awareness was one of the best ways to combat scammers and help Australians protect themselves against scams and identity theft.

"Scammers thrive on uncertainty and misinformation when it comes to the use of the **nbn** brand to access people's computers to steal information or push for unnecessary payments. This is why it is critical that we continue to educate the community about how they can protect themselves and others from being scammed.



“**NBN Co** is a wholesaler and does not make unsolicited calls to sell products, request remote access to computers through programs like Team Viewer, ask you to purchase gift cards in lieu of cash payments, threaten to disconnect your services, or request personal or financial details.

“This week, our teams will be concentrating on arming residents, and particularly those who help the vulnerable in our community, with the information on what to look out for and what to do if they suspect they have been contacted by a scammer.

“The team at **NBN Co** is committed to empowering the community with knowledge, education, and information to help protect our loved ones from these insidious scams.”

**ACCC Deputy Chair Delia Rickard:** “Scammers are increasingly using trusted brands like NBN to trick unsuspecting consumers into parting with their money or personal information. Australians lost more than \$900,000 from NBN impersonation scams in 2019 with the highest number of reports and losses coming from people aged 65 years and older.”

Details on the **nbn** Scam Awareness sessions can be found on the [nbn Facebook page](#). If you would like to book a one-on-one or group scam awareness session with an **nbn** representative, email [nbnsessions@nbn.com.au](mailto:nbnsessions@nbn.com.au)

#### **NBN Co's top tips for protecting against scammers:**

- Visit NBN Co's website at [www.nbn.com.au/scamadvice](http://www.nbn.com.au/scamadvice) for information on how to identify and avoid potential scammers or for advice if you suspect you have been scammed.
- Remember **NBN Co** will never call and ask to access your computer or advise that you're going to be disconnected. NBN Co is a wholesaler, which means it does not sell phone or internet services directly to the public. People need to contact their preferred phone and internet provider in order to make the switch.
- Never give an unsolicited caller remote access to your computer or devices via the installation of programs, such as Team Viewer.
- NBN Co does not make automated calls, such as robocalls, to advise of disconnections to **nbn** or existing copper phone line services. Do not engage with these calls.
- Do not share your financial information (i.e. bank, credit card or gift card details) or personal details with an unsolicited caller or door knockers trying to seek payment for a service over the **nbn**<sup>TM</sup> network.
- If in doubt, hang up and call your retail service provider on their official customer service centre number to check if the call is legitimate. Do not use contact details supplied by the caller.

**ENDS**

## **Media enquiries**

<b>Christina Patsias</b>	<b>NBN Co Media Hotline</b>
Email: <a href="mailto:christinapatsias@nbnc.com.au">christinapatsias@nbnc.com.au</a>	Email: <a href="mailto:media@nbnc.com.au">media@nbnc.com.au</a>
Phone: 0410 443 349	Phone: 02 9927 4200

