Media release

Embargoed until 12am Thursday 7 May 2020

NBN Co reminds Australians: 'beware of scams'

NBN Co is reminding Australians to be extra vigilant about their online security, with a marked increase in predatory scammers attempting to steal personal details and commit fraud.

With Australians working, studying, shopping and socialising online during the COVID-19 crisis, scammers are increasing their efforts to steal people's personal or financial details. Similarly, scammers are using people's reliance on connectivity at this time to mislead people into thinking that their **nbn** service will be disconnected if they do not provide a 'technician' with online access to their computer.

Working remotely also raises new security concerns as most people adjust to working outside traditional office environments.

NBN Co's Chief Security Officer, Darren Kane, said: "As we spend more time online, it is important we do not become complacent when it comes to online security as scammers prey on human emotions, like fear and uncertainty, to trick people.

"Unfortunately, in times like this, phishing emails and scams soon follow as they try to take advantage of the disruption and uncertainty. With scammers increasing their efforts to use COVID-19 to steal people's personal or financial details, we are starting to see the emergence **nbn** related COVID-19 scams, so we are working with agencies like Scamwatch to continue to monitor the situation and alert the community.

"We want to remind everyone to never give an unsolicited caller remote access to your computer or devices via the installation of programs such as Team Viewer or share any financial information or personal details with someone they don't know.

"Working remotely means you are likely to be in a different environment than your usual office location, so it is important to not get complacent when it comes to the security of work devices and documents.

"It is important to not click on the links or attachments in suspicious emails and never respond to unsolicited messages. This is even more important for all of us that are working from home, as scammers are on the hunt for ways to get access and disrupt home and corporate networks.

NBN Co's top tips for working securely at home:

- Protect your work laptop or devices by not leaving them unattended in unsecure areas and locking the screen when you are away from the device.
- Do not allow family to use your work devices or passwords as they could accidentally erase or modify important work information, or unknowingly infect your device.
- Protect your home wireless network with a password and change the default administrator password on your home router using the instruction guide for your router.
- Never reuse passwords – if one site is compromised then others are too. Consider a password manager if you're finding it complicated to keep track of your passwords.

- Devices should never be left where others can see them (e.g. inside a car if you decide to duck down to the shops, or visible within a room if someone is walking past a window at street level.)
- Shred documents to dispose them securely. If you do not have access to a shredder, store the documents safely until you can return them to work and dispose of them in secure bins.
- It is best to avoid using free Wi-Fi hotspots for work-related business. These are often unsecured and the data you transmit can be snooped on by others.
- If possible, enable multi-factor authentication (MFA) whenever possible. MFA uses your password, but also adds a second step, such as a code sent to your phone or an app that generates the code for you as an extra layer of security.
- Keep personal information safe by installing the latest software and updating app to protect your personal devices from the latest threats.

NBN Co's top tips for protecting against scammers:

- Visit NBN Co's website at 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** 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 an **nbn**™ service.
- 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