

[Subscribe](#)[Past Issues](#)[Tr](#)[View this email in your browser](#)

Scamwatch radar alert

Watch out for NBN scams

Dear radar subscriber,

The ACCC is warning the community that scammers are pretending to be from NBN to con victims out of their money and personal information.

Scamwatch has received 316 complaints this year about scammers impersonating NBN with nearly \$28,000 reported lost.

“Scammers are increasingly using trusted government brands like NBN to trick people into falling for scams. Their goal is always to either get hold of your money or personal information,” ACCC Deputy Chair Delia Rickard said.

The three common scams reported to Scamwatch that involve scammers impersonating NBN are:

- signing victims up to fake accounts – scammers will ring victims to ‘connect’ them to the NBN network for a low price. They will often demand payment be made through iTunes gift cards
- gaining remote access to computers – scammers pretending to be from NBN will call a victim with claims there are problems with their computer. The scammer uses this ruse to gain remote access to the victim’s computer to steal valuable personal information, install malicious software or demand payment to fix ‘problems’ they have discovered
- phishing – scammers impersonating NBN will call victims to steal valuable personal information like their name, address, Medicare number, licence

number. The scammer may tell the victim they're entitled to a new router, for example, and say they need these personal details to confirm the victim's identity.

"Australians over 65 are particularly vulnerable to this scam with fraudsters using phone calls to target their victims," Ms Rickard said.

"NBN will never phone you out of the blue to try to sign you up to a service over its network. NBN is a wholesaler meaning they don't sell direct to the public. If you get an unsolicited call like this, it's a big red flag that you're dealing with a scammer," Ms Rickard said.

"NBN will also never call you to remotely 'fix' a problem with your computer, or to request personal information like your Medicare number or your bank account numbers. Don't listen to the reasons they give you for needing this information."

"Finally, if someone ever asks you to pay for a service using iTunes gift cards, it is 100 per cent a scam. Legitimate businesses, especially those like NBN, will never ask you to pay for anything in this way," Ms Rickard said.

People can protect themselves by following some tips:

- If you're ever in doubt about contact you've had from someone saying they're from NBN trying to sell you an internet or phone service, hang up the phone and call your retail service provider to check if the person calling is a fraud.
- You can only connect to the NBN network by purchasing a plan through a phone and internet service provider. Go to [NBN's website](#) to check if your home or business address is able to connect to the NBN network and see which phone and internet providers are available in your area.
- Never give your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.
- Never give an unsolicited caller remote access to your computer.

If you think you have provided bank account or credit card details to a scammer, contact your bank or financial institution immediately.

Further information is available at www.scamwatch.gov.au.

@scamwatch_gov



Report a scam

Follow us on Twitter



You have received this email because you have subscribed to receive Scamwatch radar alerts issued by the Australian Competition and Consumer Commission. You can [view more news & alerts](#) on the Scamwatch website.

If you have any doubts about an email's source, verify the sender by independent means - use their official contact details to check the email is legitimate before clicking on links or opening attachments.

Copyright © 2017 ACCC, All rights reserved.

[Update subscription preferences](#) [Unsubscribe from this list](#) scamwatch.gov.au acc.gov.au