What is a scam phone call?

Telephone-based scam callers often claim to be from well-known organisations such as NBN, the Government, or other brands or organisations you're likely to have heard of.

These scam callers will often try to convince you of the urgent need to follow their instructions. Sometimes they will try to convince you to give them access to your computer remotely, such as when pretending to be an NBN employee. Often, they will apply inappropriate pressure, including threats and potentially inappropriate language, as part of their scam.

What to look out for:

- Calls from people impersonating employees from well-known organisations, such as the Government, or familiar brands and companies.
- Calls seeking financial details, such as your credit card or banking details, in order to process a refund or other 'overpayment'.
- Call quality may be poor, and the caller may be difficult to understand.
- Callers which attempt to apply a lot of pressure, urging you to take immediate action to address a problem.
- Calls offering to place a number on the Do Not Call Register for a fee. This is a free service.
- Callers advising that your computer has a virus or is attacking others.

Example of scam phone calls

- Calls imitating the Australian Federal Police that require your assistance to help them track down criminals and partake in criminal investigations. In these calls you're often asked to transfer money overseas using international money transfer services.
- Calls asking for bills to be paid via prepaid gift cards – such as iTunes and Westfield – on behalf of a credit agency representing the Australian Taxation Office (ATO).
- Calls imitating support desk staff looking to access your computer by pretending to know your CLSID. This is a non-unique identifier which scammers try to pass off as something only a legitimate support person would know.

What to do next:

- If you're not sure that the person on the other end of the phone actually is who they say they are, hang up and call the organisation by using their official published contact details.
- Do not share your personal information, credit card or online account details over the phone, unless you made the call and the number you called came from a trusted source, such as the contact details provided on your bill.
- Do not return missed calls from numbers you don't recognise. Calling back may result in instant charges in excess of $20.
- Be wary of phone numbers beginning with '190'. These are charged at premium rate and can be expensive.
- Be careful of being tricked into calling expensive international phone numbers.
- If you think something's not quite right, just hang up.
- Call us with the details of the call so we can investigate and block if found to be a scam call
- Report the scam call to www.scamwatch.gov.au