FACT SHEET

FACT SHEET: Caller ID Spoofing

Caller ID Spoofing, sometimes known as Caller Line Identification overstamping, is when the Caller ID shows a phone number different to the one actually being used. Scammers often use this technique to increase the chance that their call will be answered, as the public has become more wary about answering calls from international or unusual looking numbers. This is because Caller IDs that are in a familiar format or appear to be coming from within our own country are much more likely to be answered.

Telcos have put systems in place to reduce the ability to spoof Government or large business numbers (1800, 1300, or 13 numbers in Australia, and 0800 numbers in New Zealand). Scammers have now shifted their attention to using mobilie phone numbers and landline numbers of small businesses and individuals.

Quick Facts

- Caller ID Spoofing is the unauthorised use of public number in a deliberate attempt to mask or mislead the receiving party about the origin of the call.
- Phone spoofing does not result in any charges to your phone account. The scammer is stealing the way your number looks and not actually calling from your account.
- You will usually see a decrease in scammers using your phone number within one to two weeks.

Prevention

Unfortunately there is nothing you can do to prevent a scammer from spoofing your number, or calling you from a spoofed number. Being on the Do Not Call Register will not assist, as this is a service used by legitimate companies and not scammers to determine who does not wish to contacted.

Detection – How will I know if someone is spoofing my phone number?

You may never know that someone is using your number. However the most common signs are:

- You receive calls from individuals stating they missed a call from you, even though you never called them.
- You receive calls from individuals accusing you of being a scammer.

Detection – How do I know if someone is calling me from a spoofed number?

The following warning signs apply for all telephone scams, even when they are not using Caller ID Spoofing:

- The caller requests you provide evidence to prove your identity.
- The caller claims to be from a Government Agency, the Australian Federal Police, or your local police. They may demand payment or assistance with a "sting" operation.
- The caller claims to be from a well known service provider, such as parcel delivery, nbn, telephone company, or streaming service.
- The caller requests remote access to your computer, phone or tablet.
- The caller requires you to take immediate action, such as pay a fine, make a payment, or give personal details to win a prize.
- The caller requests you move communication to another platform, such as WhatsApp.
- The caller threatens legal action if you do not comply with their demands.

FACT SHEET

Response – How can I make this stop?

Under the Industry Guidance Note (IGN 009) the Communications Alliance indicate that all carriers and carriage service providers are obliged to intervene when Caller ID Spoofing occurs.

- Contact your telco and advise them that your phone number is being used by scammers. Ask if they have a service in place to run a filter on your number across their telephone network. These programs usually take a few hours to run your number across their whole exchange so you may get the occasional call back from individuals who are contacted during this time by the scammer.
- If your mobile phone is with Telstra, you can use their online **Report Unwelcome Calls** form, and under "Tell us about the calls you have been receiving" write that your number has been spoofed and you are receiving unwelcome calls from people believing that you are a scammer.
- If you are not with Telstra, ask your telco if they offer a similar service.
- Place a voice message on your phone informing individuals of the issue. For example: ***"Hi, if you are calling because you believe you have received a call from me/us/our business, we have not made these calls. We have become aware that our phone number has been hijacked by scammers and being used to disguise their identity, This has been report to (insert the name of your Telco) who are in the process of stopping them."***

For additional support or information, contact IDCARE by submitting a Get Help Form or call 1800 595 160 (Aus) or 0800 121 068 (NZ).