Scammers are constantly changing their approach, both through the technology they use and the stories they tell. Their goal is to obtain money or personal details from you. Anyone can be caught out by a scam so the best way to protect yourself is to be vigilant. Read on for our top tips on identifying scams.

Spark nz

Report it

scamhelp@spark.co.nz

0800 809 806 (weekdays 8:00am to 6:30pm, excluding statutory holidays)

For txt message scams, report them to the Department of Internal Affairs by forwarding the message to **7726**

Report to Netsafe at **netsafe.org.nz/report**

For more information and examples of scams, visit **spark.co.nz/scams**

SPA5068

Spark nz | netsafe
netsafe.org.nz

PROTECT YOURSELF FROM PHONE SCAMS

Spotting a scam

- A scammer can disguise the original caller ID with a number they choose, such as a local kiwi number. This is called number spoofing – the call is actually coming from overseas, but the scammer hopes that by disguising the overseas caller ID they will appear authentic.
- The scammer may claim they have identified a problem with your modem/computer, and offer to help by taking control of the home computer using remote access. This may be more convincing if you have had recent technical issues.
- They may know your full name, address and date of birth. This information can be found through research online, by looking in the phone book or they can buy it on the black market. You should not assume they are legitimate for knowing these details.
- Scammers may call from an international call centre with a large number of staff – it is often very noisy in the background.
- Some scam callers may ring, then hang up before you can answer. These often come from an overseas number. This type of scam is called a Wangiri 'one ring' scam. The aim is to get you to call back, so they can collect a premium calling fee.
- You're told that you've won a prize or money for a competition you haven't entered.

How to stay safe

- Be careful where and to whom you provide your personal details.
- Make sure you keep your software and anti-virus programmes up to date.
- Use a different password for all your online accounts.
- Change your passwords often and don't reuse old passwords.
- Use 2 Factor Authentication (2FA) for online accounts where it's available.
- If you can't tell if a call is legitimately from a company you do business with, hang up and call the company directly on their number listed in the phone book or their official website.
- If you receive a missed call from a number you don't recognise, ignore it and don't call back. This may be a scam designed to lure you into calling back, and being charged premium calling rates as a result.
- Be cautious about unexpected contact – even from legitimate organisations.
- Keep up to date by visiting **spark.co.nz/scams** for the latest tips on recognising scams.
- Consider getting Call Screen, a nuisance call blocking home phone available at **spark.co.nz/callscreen**.

I think I've been scammed

- If you've done anything on your computer (or another device) at their request, immediately disconnect your computer from the internet.
- If you've given out bank or credit card details, contact your bank straight away.
- Change your online account passwords for all of your devices, and if you've given access to your computer, seek assistance from a computer services company.
- Report the scam to your telecommunications provider and Netsafe.
- Let your friends and family know the details of the scam, so they can also be on the lookout.

Block unwanted calls yourself

Spark Call Screen is a home phone that gives you control over which calls you answer by letting you screen incoming calls and block those from unwanted callers. It's simple to set up and easy to use. Visit **spark.co.nz/callscreen** or your local Spark store for more information about Call Screen.