NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

OCTOBER 2024

Practical Tips on Impersonation Scams

An impersonation scam relies on an attacker pretending to be someone the victim trusts – a celebrity, a government official, a workplace colleague, or even a family member.

In recent years the sophistication of these scams has increased significantly – from simple spam e-mails to live deepfake videos with AI-generated voice and facial movements. The latest tools can generate a very convincing video from a few photos and 20 seconds of audio from a person's social media profile. Here are a few tips to help protect yourself from these types of scams:

1. Have more than one channel of communication.

It is much harder for a scammer to impersonate someone across multiple platforms or forms of media.

For example, if you get a videocall from a family member asking for money, ask them to send an e-mail too.

If someone you know has given you a phone call from an unknown number, ask them to message you on Whatsapp or another internet messaging platform.

If your CEO has sent you an e-mail ordering you to transfer money on their behalf, go to their office and confirm the request, or call them on the phone number saved in your phone.

This is called **multi-factor authentication** because you are confirming their identity in more than one way.

2. Ask a secret question.

It can be helpful to have a question that only you and the other person know the answer to. This can be particularly useful if a close friend or family is travelling, and they might reach out to you in an emergency.

Do not rely on a question that could be answered with social media research – for example, answering "what is your favourite food" with "salmon sushi" is not effective if the other person often posts photos of them eating salmon sushi online.

You can make this stronger if the answer is not guessable or does not make sense – for example, answering "what is your favourite food" with a **code phrase** "flying to the sun" will be essentially impossible for a scammer to guess.

3. Be aware of emotional manipulation.

Scammers often insist that their requests are urgent and that victims need to act fast.

Scammers can appeal to your sense of ego by making it sound like an investment opportunity is exclusive or only for a small number of special people.

Scammers can threaten our sense of safety by claiming that a victim's computer has been hacked, or that a loved one has been kidnapped.

Scammers can appeal to a sense of authority by being direct in their instructions and issuing orders.

All of these techniques are intended to compromise the victim's ability to think rationally, and to just go along with what the attacker wants. **Take a deep breath and slow down**, and ask questions if you need to.

4. Critically evaluate offers.

If something seems too good to be true, it probably is. Check other sources to see if it's legitimate – a quick google search can help verify if others have been scammed before.

If it seems out of character for someone to be promoting or asking for something, it probably isn't them.

If someone unexpectedly asks for personal information or payment out of context, question why it is necessary.

If you are in doubt, **ask someone that you trust for their opinion** – it is harder to fool two people than it is to fool one person.

What to do if you have been scammed.

If you are the victim of an impersonation scam and have lost money, you should:

a) stop all communication with the scammer – do not reply to any further messages.

b) report it to your bank or financial institution as soon as possible – there is a limited time window where they may be able to cancel a transfer or retrieve some funds.

c) report it to Police 105 and/or the government's Computer Emergency Response Team (CERT) – they can take actions to prevent others from being scammed in the same way.

d) do not trust anyone purporting to be a 'recovery agent' who promises to get your lost money back for a fee, as this is often just a further scam.

e) talk to friends and family about what happened – it can be hard, but sharing your story is worthwhile because scammers rely on people being ashamed or secretive.

The last step is very important: community resilience is stronger than individual resilience. People are much less likely to fall victim to scams when they are part of a community and can ask for help when they need it. Showing a potential scam or suspicious message to others increases the likelihood that it gets correctly identified as a scam.
We are stronger together.