

Protecting Yourself from Financial Scams

Dr. Muhammad A. Cheema
University of Otago, New Zealand

Scams in New Zealand today

\$265m

lost to scams and fraud
in one year, reported
by 12 NZ banks

3 in 4

New Zealand adults
faced a scam in the
last 12 months

1 in 4

New Zealand adults
say they have lost
money to a scam



Only about 1 in 3 victims who reported to their bank got any money back. Stopping a scam before you pay matters most.

Sources: Payments NZ Reported Fraud Monitor, via MBIE (Nov 2025); Netsafe & Global Anti-Scam Alliance, State of Scams in New Zealand 2025.

Why scammers target pre-retirees and retirees



Savings and assets

A lifetime of savings, KiwiSaver and often a mortgage-free home



Polite and trusting

Raised to be polite, so less likely to hang up on a caller



Living alone

Loneliness or a recent loss can make a friendly voice welcome



Fast-changing technology

AI voices, fake videos and new apps make scams harder to spot

“

Anyone can be scammed.

Scammers are organised criminals who do this all day. Being targeted is never your fault.

How scammers work on you



Pretend to be someone you trust

Your bank, Police, IRD or family



Rush you

“Act now or you’ll lose it all”



Stir up strong feelings

Fear, excitement, love or guilt



Ask you to keep it secret

“Don’t tell your bank or family”



Want unusual payments

Gift cards, crypto or a “safe account”



Feeling rushed, scared or excited? Stop. That feeling is the scam at work.



PART 1

Common scams in New Zealand

Eight scams to watch for



1

Fake bank calls



2

Fake texts and emails



3

“Hi Mum” messages



4

Computer “support” calls



5

**Fake officials:
IRD and Police**



6

Romance scams



7

Investment and crypto scams



8

Doorstep and charity scams

Fake bank calls



WHAT YOU MIGHT HEAR

“This is the fraud team at your bank. Someone is trying to take money from your account. To protect it, read me the code we just texted you.”

Bank impersonation reports to Netsafe more than doubled from July to August 2026.



Warning signs

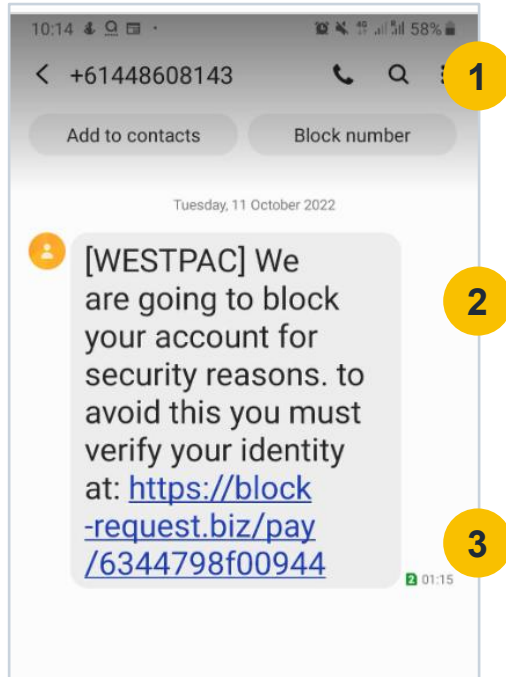
- They ask for a code, PIN or password
- They ask you to move money to a “safe account”
- Caller ID can be faked to show the bank’s number



What to do

- Hang up and call the number on your card
- Never read out a code sent to your phone

Fake texts and emails



1 A strange or overseas number

This “bank” text came from an Australian mobile (+61)

2 A threat and a deadline

“We are going to block your account...”

3 A link to an odd website

block-request.biz is not your bank’s website

Common in NZ: NZ Post “parcel on hold”, NZTA “unpaid toll”, IRD “tax refund”

✓ **Don’t click. Forward it free to 7726, then delete.**

“Hi Mum” and family emergencies



WHAT YOU MIGHT GET

“Hi Mum, I dropped my phone in the toilet — this is my new number. Can you help me pay an urgent bill? I’ll pay you back tomorrow.”

AI can now copy a person’s voice from a short clip online.



Warning signs

- A new number, and they can’t talk by phone
- Money needed urgently, to a new account
- A call that sounds just like a grandchild in trouble



What to do

- Call them on the number you already have
- Agree a family “safe word” for emergencies

Computer “support” calls



WHAT YOU MIGHT HEAR

“I’m calling from your internet provider. Hackers are using your connection. I need to log in to your computer to fix it.”

Also watch for pop-ups saying “your computer is infected — call this number”.



Warning signs

- An unexpected call or pop-up about a virus
- They ask you to install an app such as AnyDesk
- They want you to log in to your bank while they watch



What to do

- Never let a stranger control your device
- Let them in? Switch off and call your bank

Fake officials: IRD and Police



WHAT YOU MIGHT HEAR

*“You’re owed a tax refund.
Just confirm your bank
details.”*

*“This is the Police. You’re
linked to a crime.”*

Scammers have faked the Police HQ
phone number (NCSC, July 2026).



Warning signs

- Threats of arrest, fines or court action
- Payment by gift card, crypto or bank transfer
- IRD texts only come from short codes, not mobiles



What to do

- Hang up and look up the number yourself
- Use myIR directly, never through a link

Romance scams



1. Meets you online

Facebook, a dating site, WhatsApp or even a game



2. Builds trust

Daily messages and kind words, for weeks or months



3. Never meets you

Working overseas; video calls “never work”



4. A sudden crisis

Medical bills, customs fees, a ticket to visit you



5. More and more money

Or an “investment” they want you to join



Golden rule: never send money to someone you haven't met in person, irrespective of how much real it feels. Talk it over with family or a friend first.

Investment and crypto scams

How it usually works

- 1 A news story or video shows a well-known Kiwi “backing” an investment
- 2 You leave your details on a professional-looking website
- 3 A friendly “account manager” asks for a small first deposit
- 4 Your online account shows big “profits”, so you add more
- 5 When you try to withdraw, there are “fees” — and the money is gone



Red flags

- High returns with “no risk”
- Pressure to invest now
- Payment in crypto or to an overseas account
- Early investors paid with new investors’ money (Ponzi schemes)

FMA found 110 scam investment ads on Meta in one day (April 2026).

Before you invest: check first



Is the firm registered?

Search the Financial Service Providers Register online



Has the FMA warned about it?

Look at the warnings list on fma.govt.nz



Can you get it in writing?

Ask for the Product Disclosure Statement (PDS)



Get independent advice

If you don't understand it, walk away



About crypto

- Not protected like bank savings
- Prices can rise and fall sharply
- Payments can't be reversed
- No real bank, business or government agency will ask you to pay in crypto

Doorstep and charity scams



Doorstep traders

WATCH FOR

- “Your roof needs urgent repairs”
- Cash up front, no written quote
- Pressure to agree today

PROTECT YOURSELF

- Get written quotes from other traders
- You can cancel uninvited sales over \$100 within 5 working days



Charity collectors

WATCH FOR

- Appeals straight after a disaster
- No ID, cash only, or vague about the cause

PROTECT YOURSELF

- Check the Charities Register at charities.govt.nz
- Give through the charity’s own website



PART 2

Protecting yourself

Stop. Check. Report.



STOP

Don't rush. Don't click, share details or pay. A real organisation will wait.



CHECK

Hang up. Call back on a number you look up yourself. Ask someone you trust.



REPORT

Tell your bank straight away, then Netsafe or Police. Reporting protects others too.

Stop, Check, Report is the advice of MBIE's Consumer Protection team.

Your bank will never ask you to...



If anyone asks for these, it's a scam.

The same goes for IRD, Police and other genuine organisations.

- ✗ Read out a code sent to your phone
- ✗ Tell them your PIN or password
- ✗ Move money to a “safe account”
- ✗ Install an app so they can see your screen
- ✗ Hand your card or cash to a courier
- ✗ Pay with gift cards or crypto

Everyday habits that protect you



Pause before you pay

Sleep on any big or unexpected payment



Call back on a trusted number

Use your card, statement or the official website



Don't click links

Open the app or type the website address yourself



Check who you're paying

Confirmation of Payee checks the name matches the account



Lock your accounts

Strong, different passwords and two-step login



Talk it over

Family, a friend or your bank can be a second pair of eyes

New protections from NZ banks



Confirmation of Payee checks the name matches the account number



Warnings before some higher-risk payments



Unusual payments can be delayed or blocked



Scams can be reported to your bank 24/7



Banks share scammers' account details to freeze money faster

SINCE 30 NOVEMBER 2025

If your bank didn't meet these commitments, you may get some or all of your money back.

Not happy with the answer?
The free Banking
Ombudsman can help:
0800 805 950

Scammed? Act fast

1

Call your bank

Straight away,
day or night.
Every minute
counts.

2

Stop contact

Don't send more
money. Block
the scammer.

3

Report it

Police on 105
(111 if in danger)
and Netsafe.

4

Change passwords

If your ID was
stolen, call
IDCARE.

No shame: scams fool smart, careful
people every day.

Beware: anyone offering to get your money
back for a fee is another scammer.

Who to call



Your bank

Back of your card

Call first, 24/7



NZ Police

105

111 if you're in danger



Netsafe

0508 638 723

Or text "Netsafe" to 4282



**National Cyber
Security Centre**

0800 114 115

ownyouronline.govt.nz



Scam text messages

7726

Forward them free, then delete



**IDCARE (identity
theft)**

0800 121 068

Free help if your ID is stolen

Six things to remember

1

Unexpected, urgent or too good to be true? Stop.

4

Never send money to someone you haven't met.

2

Hang up and call back on a number you trust.

5

Talk to someone before you pay.

3

Never share codes, PINs or passwords.

6

If it happens, call your bank at once.



Thank You

Questions?