Helping you get Scam Savvy

bnz

Tip of the iceberg

New Zealanders are losing millions of dollars to scams each year, and this is only the tip of the iceberg.

More than half of scam victims do not report the fraud, so the true number of victims and losses is much higher.

*BNZ & Camorra consumer research July 2022 – Sample size= 846 customers

Everybody is a target

- Smart people are being scammed by smart scammers.
- Scammers are increasingly sophisticated and manipulative.
- Scammers count on you being busy and target us when our attention is pulled in multiple directions.

Education is the best tool we can arm people with to reduce harm to New Zealanders.

And that’s what BNZ’s Scam Savvy is all about. Helping New Zealanders and their businesses to be safer online.

Let’s get

What is a scam?

Scams are dishonest and deceptive attempts to trick you into giving away your money, login credentials, credit card details, or personal information.

Scams can come in many different forms from many places:

- Email
- Phone calls
- Online shopping
- Text messages
- Mail addressed to you
- Letterbox drops
- Social media posts and messages

Scams come in all shapes and sizes

These are some of the most common sorts of scams:

- Remote access - technical support
- Remote access - impersonation
- Investment
- Relationship/romance
- Online shopping
- Phishing

All of them involve people often taking on different personas in order to trick you.

Sadly, there are new scams everyday so it’s important to be aware and know how to spot the signs that something might be a scam.

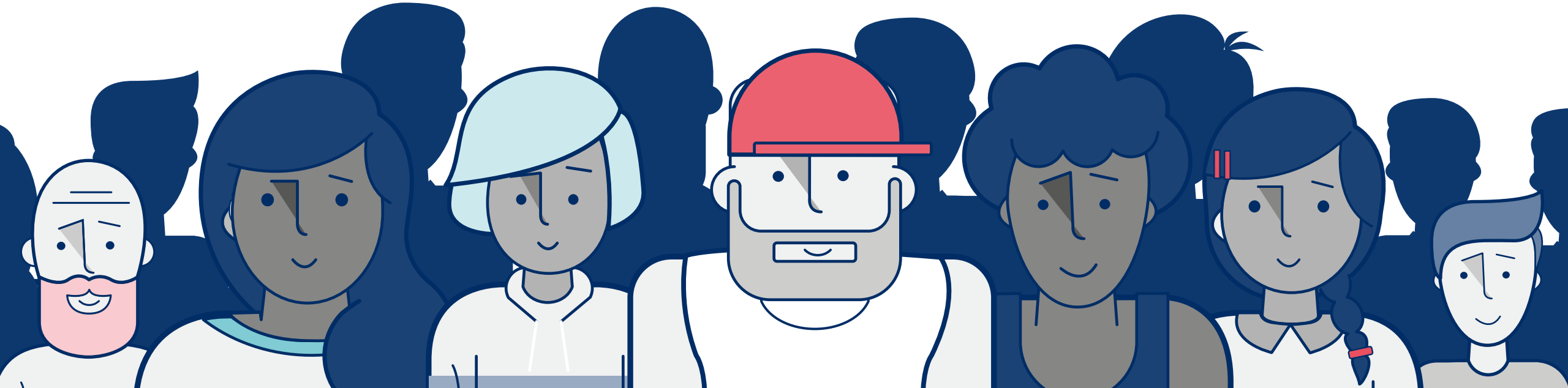
Signs that something might be a scam

- You've been contacted out of the blue by someone you don't know
- The deal is too good to be true
- The scammer wants you to take action quickly
- The scammer wants you to share personal or financial information
- The website isn't secure and there are no contact details
- It contains links directing you to confirm information or log into a service
- Poorly written communications with spelling and grammar mistakes
- The scammer has asked you to keep the question or communication to yourself

The things you already know

- You know you don’t have a long-lost uncle who has died and left you millions in inheritance
- You didn’t win USD 10 million in a lottery you didn’t enter
- A Nigerian prince isn’t in love with you and wanting to move to New Zealand to be with you

Let’s learn about the scams that are impacting New Zealanders



Remote access scam

Remote access – impersonation scam

You receive a call from a scammer claiming to be from a well-known company or organisation.

The scammer claims to have discovered 'issues' with your computer or bank account requiring urgent attention, and asks you to download remote access software.

The scammer will get you to log into internet banking to 'make sure' nobody has access to your account.

Once the scammer has access to your internet banking, they steal your money.

Remote access – impersonation scam

a scammer claiming to be from a well-known company or organisation.

Sometimes the caller will say they are from the bank's fraud team and try to enlist them to help them catch a scammer, or they will tell you they've found an 'issue' with your computer.

Ask yourself :

1. Did I initiate this call?
2. Am I a customer of the business who has called me? This could be Spark, Vodafone, BNZ, ASB, etc.
3. If not, hang up!
4. Why would an organisation that I am not a customer of contact me?
5. If in doubt, hang up!

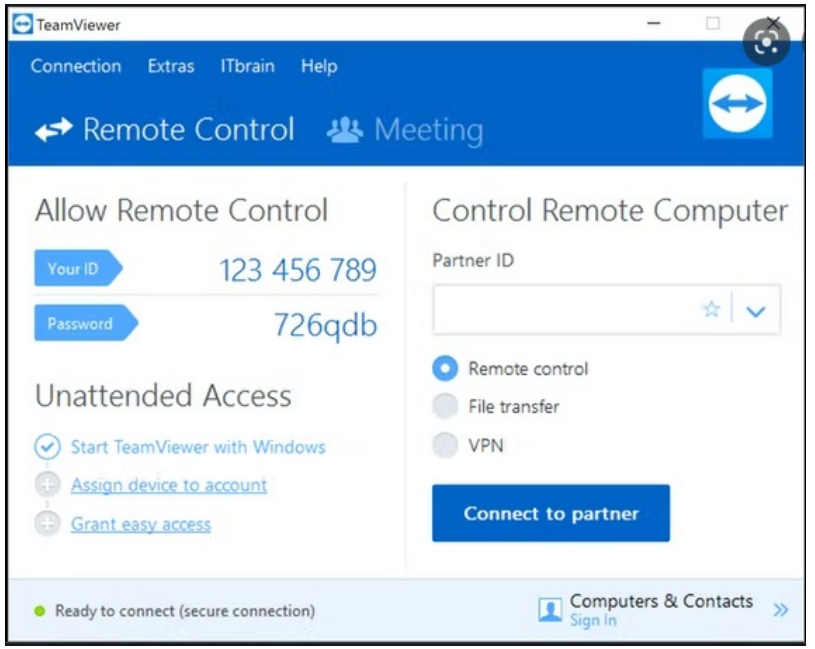
Remote access – impersonation scam

The scammer claims to have discovered ‘issues’ with your computer or bank account requiring urgent attention, and asks you to download remote access software.

The scammer will tell you they can fix the 'issue' once they have 'remote access' to your computer.

This 'remote access' programme may be called Any Desk or Team Viewer.

The scammer may ask you to turn off all other communication methods as these will ‘interfere’ with the work they need to do.



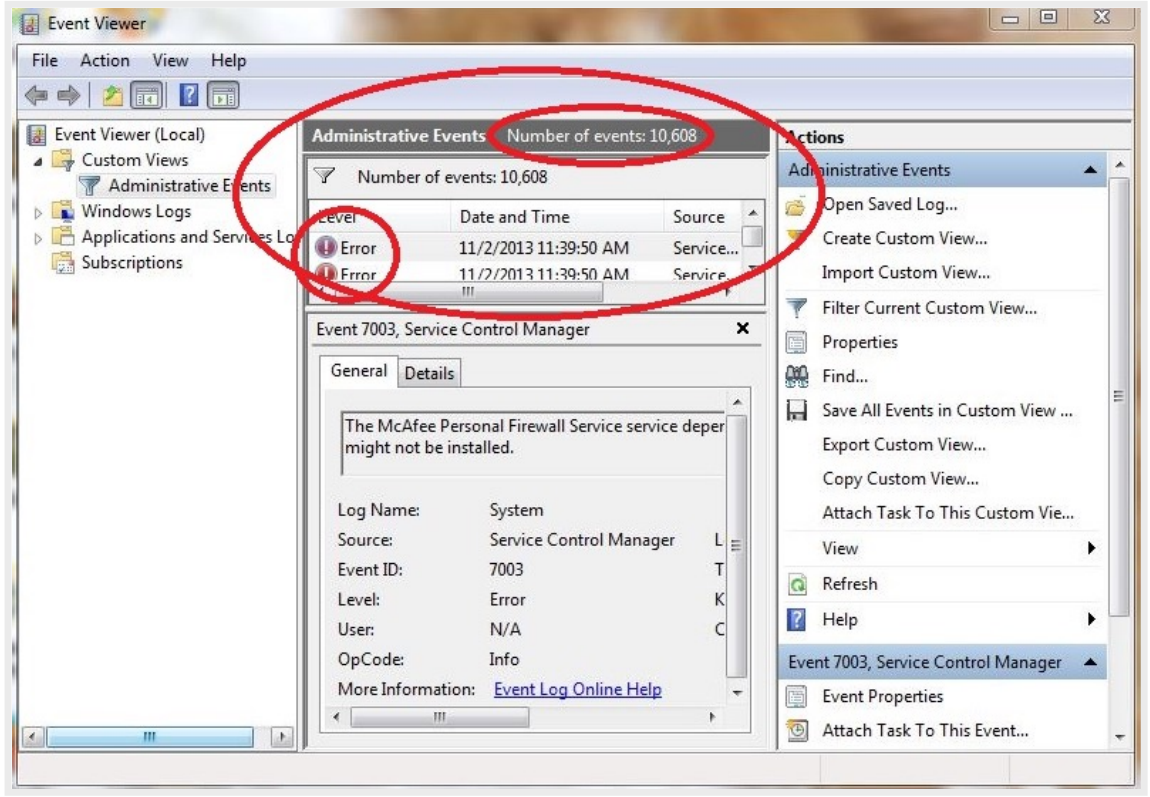
Building credibility during the call

The scammer will try to build credibility with you, this can include talking to you for hours, or showing you common computer errors, that will be on your computer that "need" to be repaired.

These errors are completely normal and expected, even on brand-new computers.

Once you download the 'remote access' program, the scammer will have full access to your computer.

Your computer screen is replicated on their screen, and they can see everything you've typed.



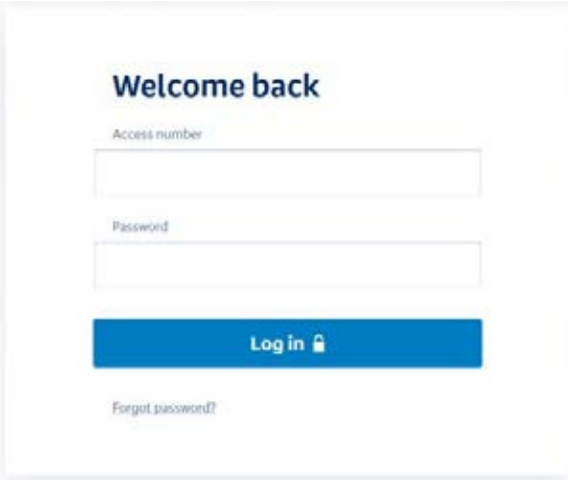
Remote Access – Impersonation scam

The scammer will get you to log into internet banking to 'make sure' nobody has access to your account.

This is where the scam happens.

The scammer will now get you to log into your internet banking to check transactions and 'make sure' nobody has had access to your account, or they'll get you to load a payment.

As well as having access to your computer, they now have full access to your bank account, and your money will be gone!



What can you do?

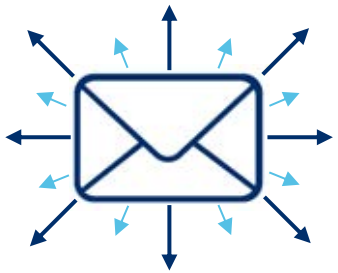
- Hang up!
- Break contact with the offender
- If you're unsure, hang up and call the company back using details you already have or that are available on their website.

If you fall victim to this scam:

- Shut down your computer – this will end the session of 'remote access'
- Contact your bank immediately

Phishing

Phishing

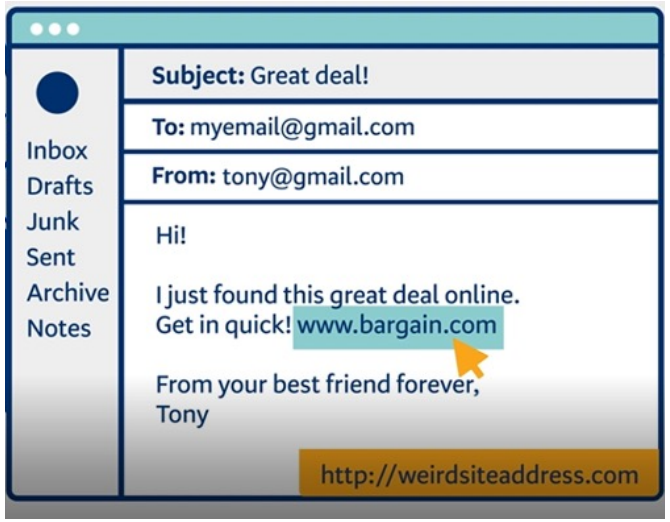


Scammer sends out an email or text in bulk, claiming to be from a well-known organisation. They request personal or financial details.

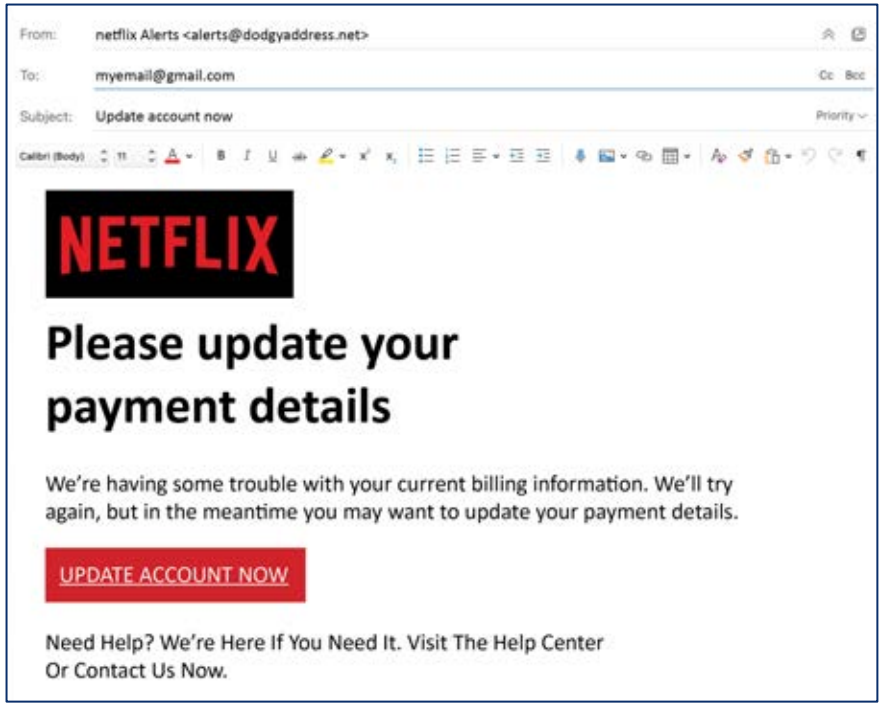
You provide the requested details, believing to be communicating with the legitimate business.

Scammer uses this information to steal your money or impersonate you.

How can I identify an email phishing scam?



Scammers hide fake websites behind real-looking links.



Scammers copy trusted brands and appear more genuine to try and capture your personal details.

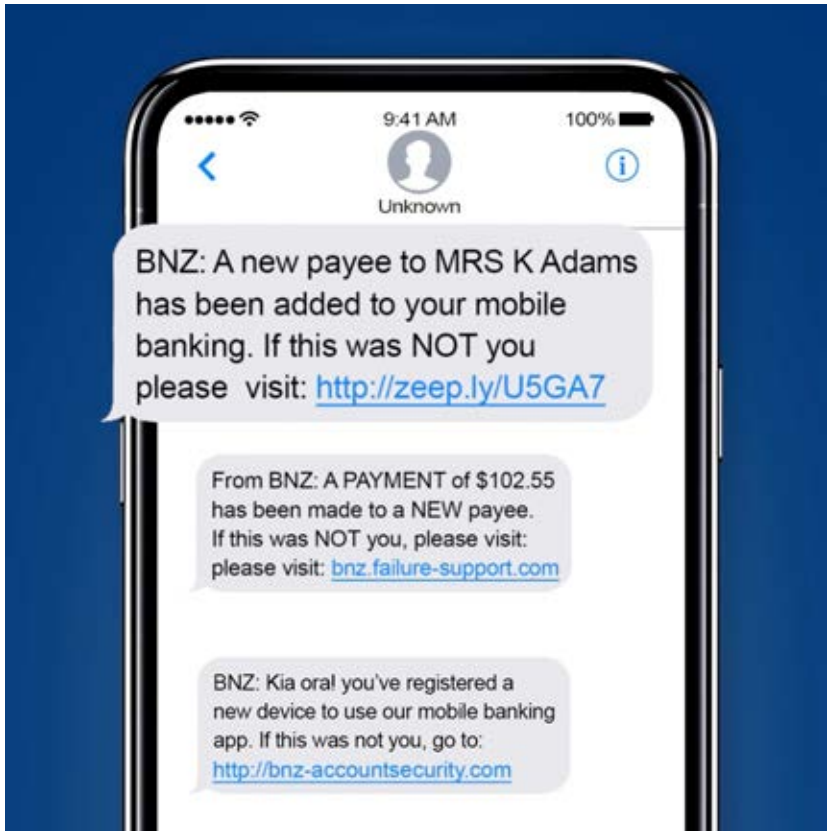
How can I identify a text phishing scam?

Text phishing is growing in popularity because they are harder to identify.

A sender name or number you don't know.

A suspicious looking link

A threat to lock you out of an account or your device unless you do something.



A message wanting urgent action from you

Request to do something unexpected like accessing a website, confirm delivery, pay for something, or accept a prize.

Phishing

What to look out for

- Be wary of urgent requests for personal information, login details, or financial payments
- Look out for emails not addressed to you personally
- Never click on a link or attachment from someone you don’t know or aren’t expecting.
- You could hover over a link (be careful not to click on it) to reveal the link’s true destination.
- On a mobile phone, tap, and hold to preview links.
- Be wary of poor spelling or grammar in emails as these can be indicators of scams

WhatsApp scam

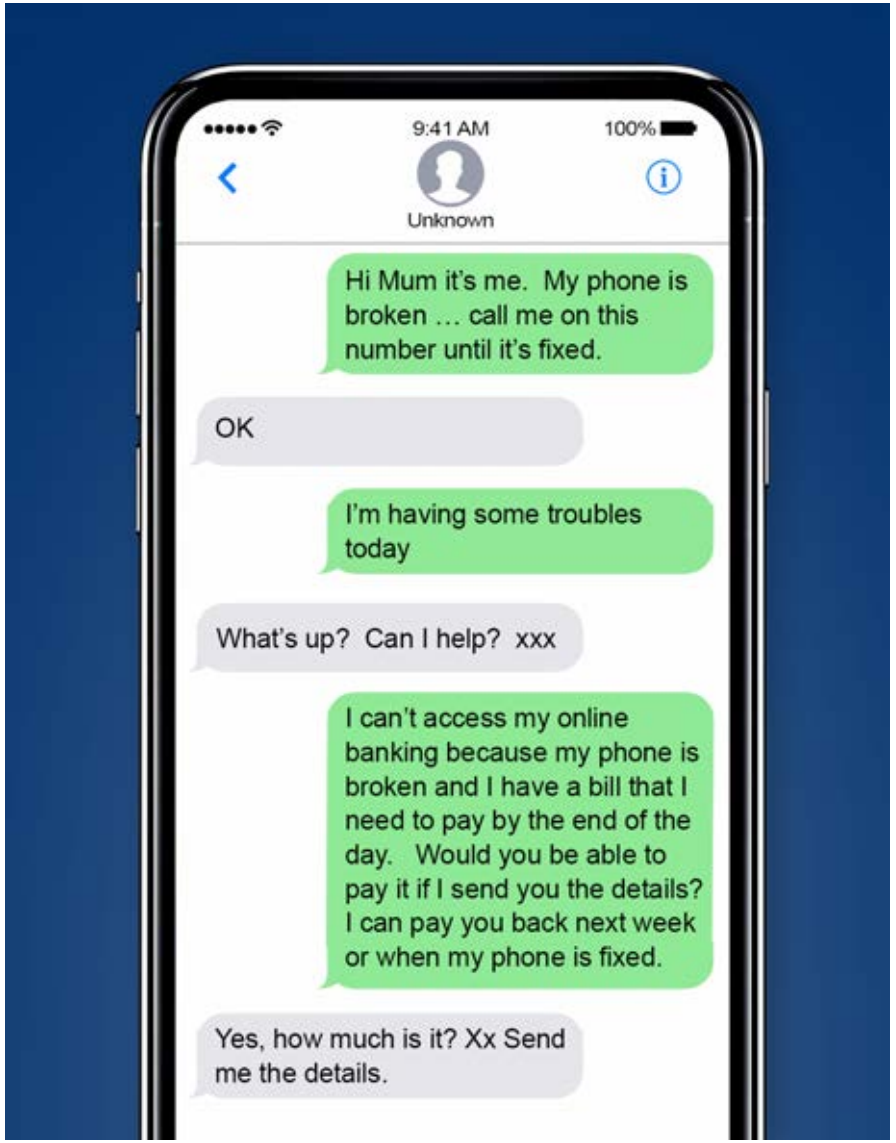
WhatsApp scam

The WhatsApp scam has become increasingly popular in 2022.

Victims of this scam receive a message from an unknown number, which claim to be a loved one who has lost their phone and got a replacement.

The 'loved one' then claims that because they have a new phone, they don't have access to their internet or mobile banking app and need help to pay an urgent bill

Victim then transfers money to an account thinking they are helping their loved one



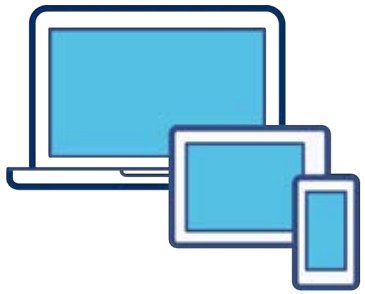
What can you do?

If someone is claiming to be a loved one on a new number and they are asking for money or something seems off, get in touch with them via other means, like a phone call or Facebook message.

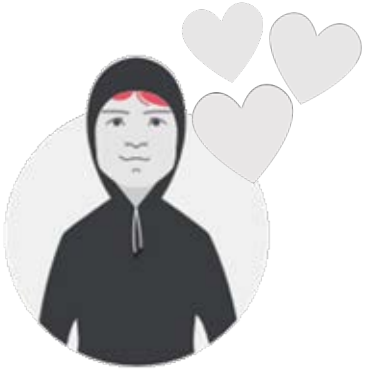
Proactively set up a code word with your close family members, which you can use to verify someone if they are claiming to be a family member.

Relationship scams

Relationship scams

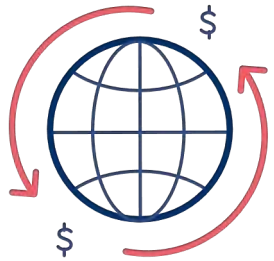


You meet someone online and form an emotional connection.



Strong emotions are expressed by the scammer within a short timeframe, attempting to gain your trust. However, it may take months for the scammer to ask for money.

Scammer slowly begins to ask for money and, once successful, will ramp up the frequency and amount they are asking for.



Scammer advises you they need someone to receive money on their behalf and then forward it to another account, usually overseas.

tinder Instagram facebook WhatsApp

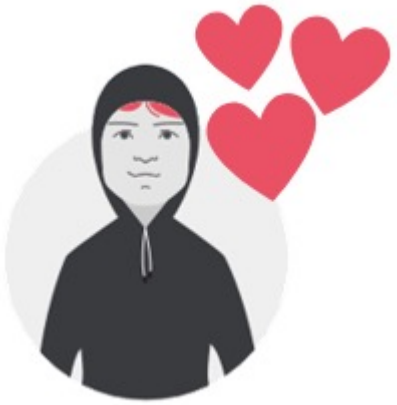
bnz

Relationship scams

What to look out for

- Strong emotions expressed within a short timeframe
- The scammer gives you excuses as to why they cannot meet in person or video call
- They've asked you to keep the relationship a secret
- You're asked to give financial assistance
- You're asked to receive money on their behalf and forward it to them
- You notice changes in communication style or being called the wrong name

Relationship scams



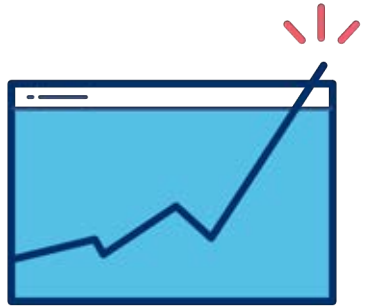
What can you do?

- Be cautious of new friend requests or messages on social media from people you don’t know
- Don’t respond to requests or hints for money
- Don’t give out banking details or send money to someone you don’t know or haven’t met in person
- Avoid giving out personal information which could be used to impersonate you
- Never agree to receive or forward funds on behalf of someone else

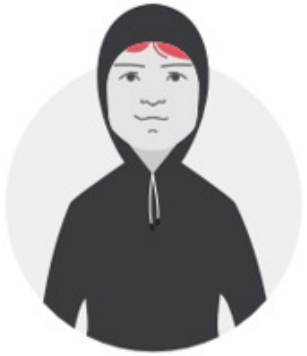
Investment scams

Investment

Cold call or advertisement online proposing an investment, including cryptocurrency, with low-risk and high returns.



You make an initial investment and, as you see your portfolio continuing to make high returns, you invest more money.

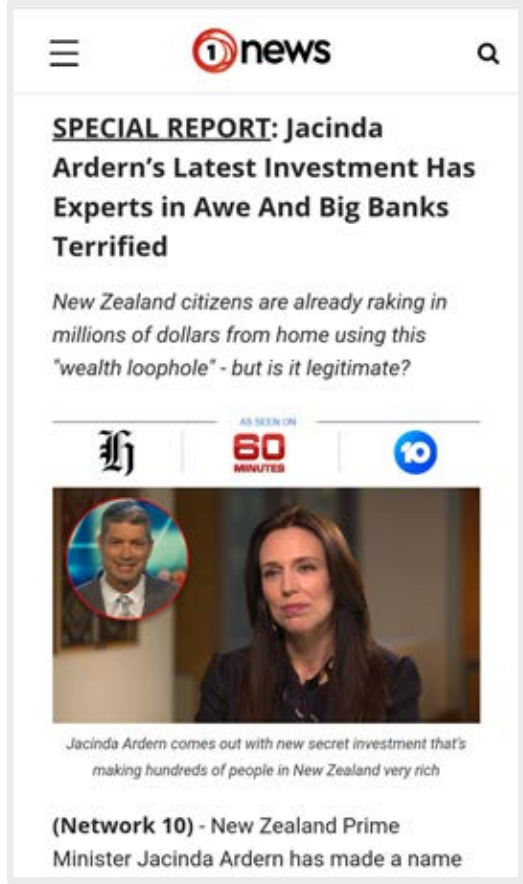


When you stop investing, or try to be paid out, your ‘broker’ will break contact with you.

Investment scams

What to look out for

- A cold call offering an investment opportunity
- An investment claiming to be endorsed by a celebrity
- You are promised an investment with very high return and little risk
- You are told an investment offer is only available to a select few
- Someone offering to invest in cryptocurrency on your behalf
- Another person in control of your computer or cryptocurrency wallet



If it sounds too good to be true, it probably is.

Investment

What can you do?

- If you receive a call offering an investment, hang up
- Be wary of celebrity endorsements of investments or cryptocurrency
- Check an investment provider’s license with the Financial Markets Authority
- Don’t allow anyone to invest on your behalf, including in cryptocurrency
- Don’t allow anyone access to your computer or your cryptocurrency wallet to make trades
- Talk through the situation with a friend or family member

Online shopping scams

Online shopping scams

You find an item online you would like to purchase, for example through Facebook Marketplace or Trade Me.

You pay for the item.

Seller never sends the item and breaks all contact with you.

Online shopping

What to look out for

- Product advertised at a significantly lower price than it’s worth.
- Seller refusing to meet.
- Newly created profile of seller.
- There may be a sense of urgency in the seller’s post or communication.
- Communication ceasing once you have made the payment.
- It’s possible the seller may ask for an upfront payment or deposit.

Online shopping scams

What can you do?

- Be wary if the seller's profile is brand new
- Check if the seller has any negative reviews
- If possible, use the payment channel on the website
- Try to avoid any arrangement asking for an upfront payment. See if you can pay when you pick the item up.
- If you're purchasing tickets to events, use official resale sites
- Be wary of offers of a free product trial where you pay for shipping only. Often by accepting the trial you may be unknowingly signing up to ongoing payments in the future.

Top tips for being

Top tips for being Scam Savvy

- Never share your login details, password, or PIN with anyone
- Avoid repetitive or sequential numbers for your PIN. Never use your birthday – it's the first thing a scammer will try.
- Be aware that your bank will never ask you to disclose your PIN over the phone
- Keep your computer and phone's security software up to date. Automate the updates.
- Avoid using public Wi-Fi for internet banking
- Don't click on links sent by someone you don't know or seem out of character for someone you do know. Hover over the links to reveal the actual site. If it doesn't seem right, call the sender using contact details you already have or that are available on their website.
- Never give someone remote access to your computer or device if you didn't initiate the call yourself
- You can also help others stay safer online by reporting any online scams you come across at CertNZ.govt.nz
- **Remember if it looks too good to be true, it probably is!**

Long and strong passwords make a difference

- Make your password long and strong: sentences are best because they're easier to remember.
- Use a different password for every online account. This way, if a scammer gets hold of one of your passwords they can't access your other accounts.
- Keep your passwords safe: using a password manager (protected by a strong password) means you only need to remember one set of login details to access all your passwords.

Password	Time to crack
Qwerty123	INSTANTLY
Sheba01	1 MINUTE
I love my cat	100 THOUSAND YEARS
l.H%kiguefjn0)9e	41 TRILLION YEARS
I love gummy bears!	4 QUINTILLION YEARS

- Don't use personal information; it's easy for scammers to find online. Likewise, don't use information available online to create password.

Source: https://www.security.org/how-secure-is-my-password/

Scammers rely on your good manners

- It is okay **not** to respond to someone you don't know
- On the phone, you don't need to speak to the caller. If you're not sure - hang up!
- On social media, be careful about over friendly people who want to get to know you fast and may have financial problems.

And remember, your bank will never call you to ask you for remote access to your computer or online banking.

Test yourself with some real life scenarios

Run a business? We have scenarios for you too.

getscamsavvy.co.nz

bnz.co.nz/security

Getting help

If you think something is a scam, and you're not sure, there are many organisations that can help, including:

- Cert NZ : www.cert.govt.nz
- Netsafe: www.netsafe.org.nz

If you think you have been scammed, contact your bank immediately.

netsafe
netsafe.org.nz

certnz

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND

New Zealand POLICE
Ngā Pirihimana o Aotearoa

bnz

Important information

The information in this presentation (Information) is provided for general purposes only. The Information is not intended to be a complete summary of how scams operate in New Zealand. If in doubt, you should contact BNZ for help or another trusted adviser.

Information must not be used for any other purpose without BNZ's prior written permission. No representation or warranty is made as to the accuracy, reliability or completeness of any Information. We don't accept any liability or responsibility for any loss you incur as a result of your use or any error or omission from the Information.

References to third party websites are provided for your convenience only. We don't accept any responsibility for the availability or contents of such websites.

Ngā mihi