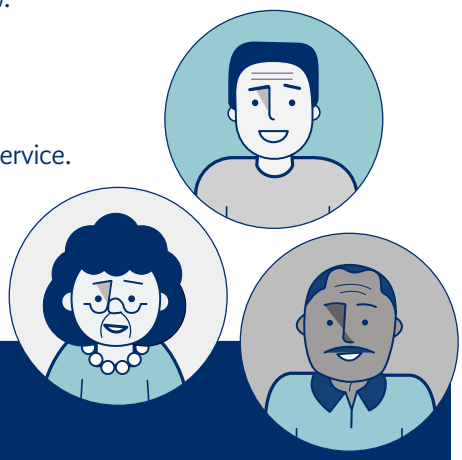
bnz

Helping you get Scam Savvy

New Zealanders are losing millions of dollars to scams each year

The tactics may vary from scam to scam, but here are the most common signs that something might be a scam:

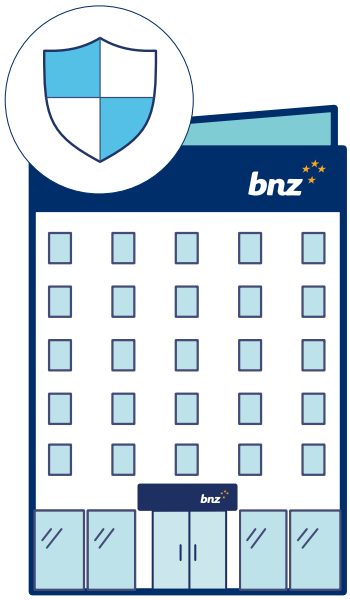
- You've been contacted out of the blue by someone you don't know.
- There is a sense of urgency to the communication.
- You are asked to share personal or financial information.
- You are sent a link asking you to confirm information or log into a service.
- You've been asked to keep the communication to yourself.
- It sounds too good to be true.



Everybody is a target

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

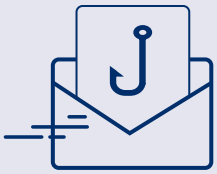
What BNZ will never do



If you get a message that looks like a scam, make sure you know what the companies you deal with, will or won't ask you to do. For example, BNZ will never:

- email or text you links to online banking and ask you to log in
- send you a text message with a link to a website, or link to call us
- ask you for information about your PIN number, bank account number, or password
- ask you to verbally share the authentication codes sent to you by text or email, even with a BNZ staff member
- ask you to transfer money to help catch a scammer or a bank employee who is scamming customers
- send you a text message about account issues with a link to log in
- ask you to download software to access your Internet Banking remotely
- use international phone numbers to call or send you notifications.

Phishing



How does it work?

Scammer sends out an email or text in bulk, claiming to be from a well-known organisation. They ask you to click on a link to provide personal or financial details.

After clicking the link, you provide the requested personal or financial details, believing you are communicating with the legitimate business.

The scammer uses this information to steal your money and impersonate you.

What to look out for

- Urgent requests for personal information, login details, or financial payments.
- Emails or text messages that are not personalised, or contain no identifying details, when they usually would.
- Emails or text messages that are not personalised, or contains no identifying details, when it usually would.
- A link or attachment from someone you don't know or aren't expecting.
- You have no dealings with the organisation or company claiming to contact you.

What you can do

- Double check the email address or phone number of the sender with previous communications or via their official website.
- Never click on a link or attachment from someone you don't know or aren't expecting.
- 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 urgent requests for personal information, login details, or financial payments.
- Report phishing emails to Cert NZ. For text phishing, forward the text to Department of Internal Affairs on 7726 (SPAM).

Investment

How does it work?

You enter your details in a fake website for someone to contact you. You are expecting the scammer's call.

After an initial investment, your portfolio shows high returns, and you invest more money.

When you stop investing, or try to access your returns, your 'broker' will break contact with you.

What to look out for

- A cold call or social media message offering an investment opportunity.
- An investment claiming to be endorsed by a celebrity.
- A promise of an investment with very high returns and little risk.
- Claims the 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.

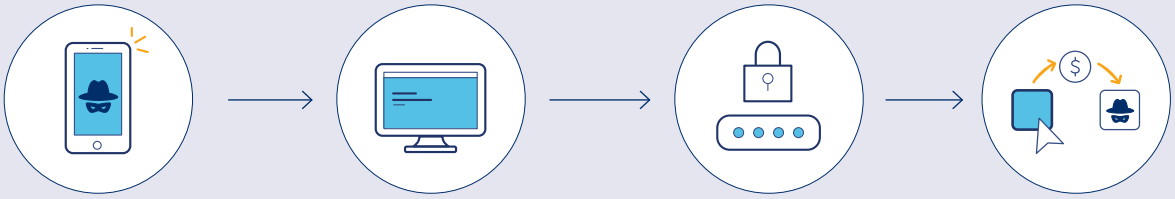
If it sounds too good to be true, it probably is.

What you can do

- If you receive an unsolicited call or message offering an investment, hang up or delete it.
- Be wary of search engine results for investments or term deposits that are sponsored advertisements.
- Be wary of celebrity endorsements for 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.

Impersonation

How does it work?



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

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

2. The scammer asks you to transfer money to keep it safe or catch a hacker OR asks you to withdraw cash to help with an "investigation". You may also be asked to purchase prepaid cards.

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

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

What to look out for

- An unexpected call from a company or organisation you already have dealings with. This is usually your internet provider or bank.
- Calls from Police or your Bank asking you to help them catch a scammer or thief within the bank.
- Being told there is an issue with your bank account or computer, for example, unauthorised payments or someone is 'hacking' you.
- Someone wanting to take remote control of your computer. This means they can control your computer from a different location.
- You are asked to turn off all other communication methods as these will 'interfere' with the work they need to do. The real reason they ask this is so the bank can't reach you if they notice anything unusual.
- You may be given a cover story in case you do need to contact the bank.

What you can do

- BNZ and the Police will never ask you to withdraw or transfer money to help catch a scammer or bank employee who is scamming customers.
- Do not feel obligated to respond to questions or comply with instructions.
- If you're unsure, hang up and call the company back using details you already have or that are available on their website.
- Never let someone you don't know remotely access your computer or any other device.
- If you have allowed someone remote access to your device, end the session by turning it off. Contact your bank immediately.
- Take your computer to a technician to be checked before using again.

Online shopping

Selling online - How does it work?

You list an item for sale. An illegitimate buyer hits 'Buy Now' on the item you're selling.

You'll receive an email asking you to finalise the sale by confirming your details. There'll normally be a button for you to click to continue. You're then taken to a fake website, asking for your credit card details, internet banking login, Trade Me login or other personal details. Even though they claim there is no cost to you.

You send the item. You've lost your personal and credit card details and the item.

What to look out for

- Newly created profile of buyer.
- No questions asked about the item you are selling.
- Asking for a third party to be involved i.e. a courier to pick up the item or a provider for payment e.g. PayPal.
- They might overpay you for the item.

What you can do

- Be wary if the buyer's profile is new.
- Review feedback of the buyer. Do they have negative reviews or are there no feedback reviews at all.
- Never engage a third party.
- Do not enter your details into a website for parcel collection or courier.

Online shopping

Buying online - How does it work?

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.

What to look out for

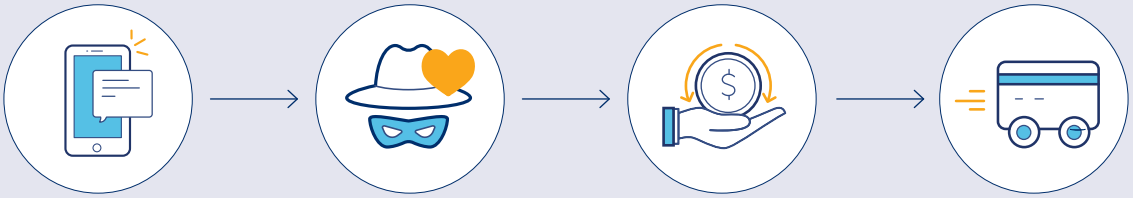
- Product advertised at a significantly lower price than its worth.
- Seller refusing to meet.
- Newly created profile of seller.
- There may be a sense of urgency in the seller's post or communication.
- Communication ceasing once you have made the payment.
- It's possible the seller may ask for an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

What you can do

- If possible, use the payment channel on the website, rather than paying by internet transfer or cash.
- 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, use official resale sites instead.

Relationship

How does it work?



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.

The scammer slowly begins to ask for money or encourages you to make an investment with extraordinary returns. They will continue to ask for money or investment funds during your relationship.

The scammer may ask you to receive money on their behalf, and forward it to another account.

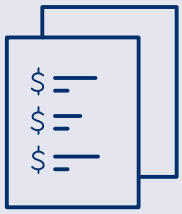
What to look out for

- Strong emotions expressed within a short timeframe. This is an attempt to gain trust.
- May have an uncommon profession or work overseas.
- Gives you excuses as to why they can't meet in person or video call.
- They have asked you to keep the relationship a secret, even from family or friends.
- Being asked for financial assistance, or to receive money on their behalf and forward it to them.
- Changes in communication style, being called the wrong name, or a generic term of endearment, for example, 'dear' or 'sweetheart'.

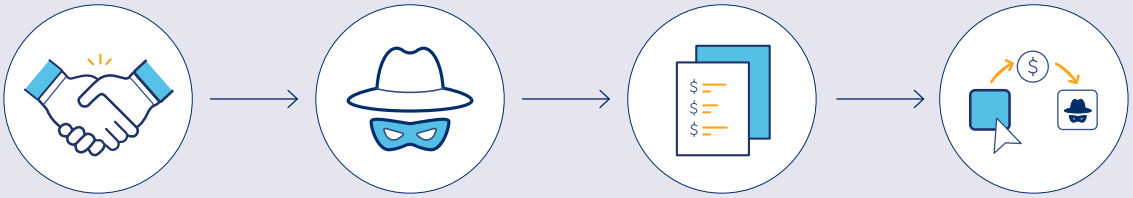
What you can do

- Be cautious of new friend requests or messages on social media from people you don't know.
- Be wary if someone is using a New Zealand based dating app, even though they live overseas.
- If it's an option on the dating site or app you are using, only communicate with people who have a verified profile.
- 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. This may make you a money mule. It is a crime.

Invoice



How does it work?



You and a legitimate supplier or business have an established relationship.

Business or supplier's email is hacked.

The scammer updates the payment account on a tailored invoice. This is then sent to you to pay.

You pay the fraudulent invoice. It may be some time before the fraud is detected.

What to look out for

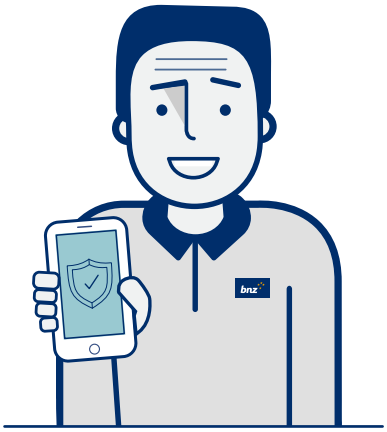
- Business or supplier asks for payment to be made to a different account number than usual.
- The altered invoice usually comes from someone you have dealings with for higher value transactions, such as, lawyers, real estate agents, builders, etc.
- May involve a sense of urgency.
- Overly formal or unusual wording for the request.
- The tone of the email doesn't match what you're used to, or the person signs off the email with a different version of their name. For example, someone who always signs off their email as 'Bob' suddenly signing off as 'Robert'.

What you can do

- If you receive updated bank account details for a business, call them directly to confirm.
- Don't use the contact details on the invoice or in the email as these may have been changed by the scammer.
- Double check whether the tone or communication style of the email matches what you expect from that person or business.

Protecting your personal information and money is our top priority

- Our fraud experts are working 24/7 to protect your personal information and money, and they are available when you need specialist help.
- Our frontline teams are trained to help identify scams and provide Scam Savvy education.
- If you need help to manage the financial consequences of a scam, we have people to help you work out the best way forward.
- Find out more at **bnz.co.nz/onlinesecurity**



To help every New Zealander feel safer online, we've created a range of tools designed to help you learn how to confidently identify and avoid scams.

For practical tips on how to be safer online, visit **www.getscamsavvy.co.nz** for scam alerts, quizzes and downloadable presentations you can share with your friends, whānau or community groups.

You can help others be safer online by reporting any scams you come across

If you've received an email or text and have provided your personal banking information, call us immediately on **0800 735 901** (international **+64 4 479 5901**).

Once you've reported the scam to BNZ, report your case to NZ Police (105) **105 Police Non-Emergency, New Zealand Police**.

BNZ related phishing: **phishing@bnz.co.nz**

We have dedicated Cyber and Fraud teams who investigate and manage each report on a case-by-case basis.

For other support

Forward phishing texts to:
Department of Internal Affairs (DIA) 7726 (SPAM)

Report spam texts or email to:
Department of Internal Affairs www.**dia.govt.nz**

Report investment scams to:
Financial Markets Authority www.**fma.govt.nz**

Report cyber security issues to:
Cert NZ 0800 237 869 **www.cert.govt.nz**

Scam Savvy

Ngā mihi

bnz

14576 09-24