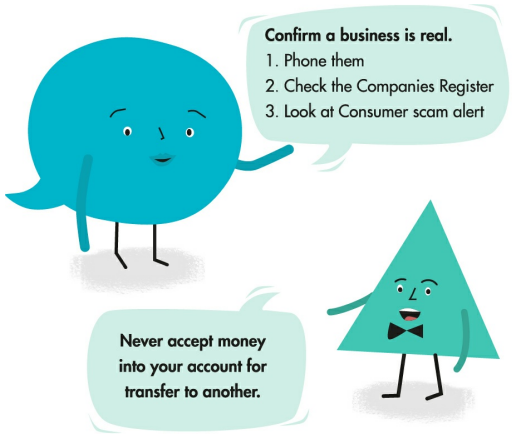
Fraud & Scams

Following some basic precautions will keep your money safe from increasingly sophisticated scammers.



Scams targeting bank customers are becoming more sophisticated and more common. Despite that, following some basic precautions will keep your money safe from scammers. If you do become the victim of a scam and complain to us, our job is to determine whether your bank is liable for the loss.

Ways to bank safely

You always need to be on your guard when it comes to banking and money matters. That doesn't mean being suspicious or paranoid. Rather, it means exercising care and maintaining a healthy scepticism towards individuals or companies when you're online. We recommend you take the following precautions:

- Never disclose PINs or passwords or save them in any way – including in your internet browser settings or in disguise.
- Investigate recipients to ensure they are genuine before sending funds.
- Check with someone independent and trustworthy before you commit to anything.
- Never accept money into your account for subsequent transfer to others.
- Check your accounts regularly to ensure money is going to the right places.
- Contact your bank immediately if you suspect you have been scammed.

In this guide, we explain some common scams targeting banking customers and banks' obligations to scam victims. Please see the Commission for Financial Capability's **Little Book of Scams** for more information about these and other types of the scams.

See our **scam prevention tip sheet**, which has lots of information to help you steer clear of current common scams.

When scammers trick you into sending money

Scammers can trick you into sending money to them in various ways. A common way is to offer investment services that may not deliver expected returns or may be a sham. Another is for an online friend to seek financial help. Losses from such scams can run into tens – or sometimes even hundreds – of thousands of dollars.

Always be careful if someone you don't know or have met only online asks for money. It can seldom be recovered. Your bank is very unlikely to be liable for losses you suffer if you give it instructions to send money to someone and you later find out that the individual was a scammer. It is your responsibility to ensure the legitimacy of the person you are sending funds to, but banks may be liable if they fail to detect warning signs of a scam.

Online purchase scams

Online purchases are a convenient way to shop, but this convenience comes with a degree of risk because it can be difficult to determine the identity and genuineness of the person you are dealing with. Some scams involve online sales in which the seller has no intention of ever providing the service or goods, or the buyer sign up for a small fee, only to find later charges of significant amounts.

If you have bought an item through a website with a debit or credit card, but the item does not arrive or the service was not what you agreed to, speak to your bank about the possibility of "charging back" the transaction. See our quick guide on **chargebacks** for more information about this process.

Be careful when arranging private sales online with people you don't know, such as through trading sites or social media. If a private sale turns sour but you paid through internet banking, it may be very difficult to recover the payment.

Fake cryptocurrency, foreign exchange investments

The popularity of cryptocurrency and foreign exchange trading and investments has led to numerous fake online investments. These are often advertised on social media – and sometimes with trusted New Zealand personalities purporting to endorse them. These services operate almost exclusively online, making it hard to differentiate between legitimate and scam services.

These scams typically involve transferring funds to an online platform to trade in currencies or stocks. However, online trading of this nature can be high risk and you can lose all invested funds. In some cases, the platform itself may be fake and you may be shown false trading records to prevent you from realising your funds have been stolen.

Find out something about the company or individual you are dealing with. Do an internet search, look for reviews, ask for a physical address you can check, and look up the company on the **Companies Register**. You can check whether it appears on the Financial Market Authority's **warning and alert page**, and read its **advice** on how to protect yourself from being scammed. We also suggest seeking advice from an authorised financial adviser before making any significant investment.

Read about how Jennifer lost funds in an investment scam in this **case note**, and why we thought her bank wasn't aware she was being scammed.

Romance scams

With online dating commonplace these days, scammers may seek to befriend or romance you with the intention of obtaining funds from you. Once the relationship is established, the online friend may tell you an unforeseen event or tragedy has happened and he or she needs financial assistance, or needs funds to travel to see you.

Victims of this scam are often older, have less experience with using the internet, but have significant savings, which a scammer can quickly drain. Victims may be emotionally involved with their scammer, making it challenging to break the spell.

See this **case note** about how Harper lost funds to an online friend and how her bank failed to detect warning signs of fraud.

Invoice scams

In this type of scam, a scammer hacks the email account of a legitimate company and alters invoices to request clients pay funds to a different account. Since the email and invoice look legitimate, these scams are hard to spot but simple checks can reveal them.

If you receive a request to pay a new or different account, we recommend you confirm the payment details using another form of communication (such as by phone). You may not be communicating with the person you imagine via email and a quick phone call can foil such deception.

See how Pierce lost funds in this **case note**, and why his bank wasn't responsible for his loss.

Recovery room scams

Recovery room scammers target you if you have already lost funds in a scam, whether their own scam or another fraudster's scam. They contact you and pretend they can help you – for a fee – get back the money you lost in online investment and trading scams (see above). They seldom explain how they will recover the money, they generally ask for their fee upfront, often by credit card, and they can end up debiting very significant amounts to your card.

Once you pay upfront fees to a recovery room scammer, you are unlikely to get any money back from the previous scam and you won't hear from the scammer again. Getting any money back from either scam can be very difficult.

If you've been a victim of a scam, be very careful about paying someone to help you get your money back. The person may not be genuine, and you may well be at risk of further losses. Instead, talk to your bank, the police or us – for free.

See our quick guide on **recovery room scams** for full details.

When scammers gain access to your accounts

Scammers also try to trick you into giving out personal information such as bank account numbers, passwords

and credit card numbers, or giving access to your computer or mobile phone. This type of scam often takes the form of contact from what appears to be a company you have a relationship with, such as an email from your bank or a call your telecommunications provider. Professional scammers aren't the only ones to try to gain unauthorised access to bank accounts. Sometimes people known to victims impersonate them to gain access to their bank accounts.

Under the Code of Banking Practice, banks agree to reimburse fraud losses if your card or electronic banking was used without your authority and you:

- weren't dishonest or negligent
- complied with the bank's terms and conditions
- took reasonable steps to protect your banking.

Even if you failed to meet these conditions and therefore disqualified yourself from protection under the code, the bank may still be liable if it did not keep the way you bank secure.

Email scams

In this scam, victims will typically receive an email from what looks like their bank or other trusted organisation saying they need to confirm some personal details, usually their username and password. It will contain a link to a website that looks like the organisation's but is fake. After victims enter these details, scammers can steal personal information or access accounts to steal money.

Be *extremely* wary of emails that ask you to confirm your personal details. Don't click on links within any email if you have the slightest suspicion about its authenticity. Simply delete the email. If you need to go to the organisation's website, type the address into your browser.

Remote access scams

Scammers may also make phone calls pretending to be your bank or telecommunications provider or a government department. They may ask you to turn on your computer and download software. They will tell you the software is to help you, but the software gives them access to everything on your computer. A scammer who has gained access to your computer may be able to steal money from your bank accounts. Be very cautious about unsolicited phone calls, no matter how plausible the caller sounds.

Be alert to requests from service providers that fall outside the scope of the services they offer. For example, your telecommunications provider is not able to provide information about your banking security, so it will not ask you to log into your internet banking when offering you technical support. If someone asks you for remote access to your device, you should call the company back on its publicly listed number before continuing. If the company did not contact you, you should notify your bank immediately so it can check your accounts are secure.

Read our **case note** about how Ingrid got taken in by this scam, and how we determined what happened.

Impersonation scams

The people you have relationships with – friends, family members, carers, employees and so forth – often have the means to potentially scam you. Such people can do this by stealing cards, overlooking PINs being entered (see our quick guide on **cards and PINs)** and using impersonation to reset internet and phone banking details. Take care

when accessing your banking around others and check your bank accounts regularly. If you need help managing your banking, put appropriate arrangements in place – see our quick guide on **access to banking** for more information about banking support.

See how Boyd's step-son impersonated him in this **case note**, and how we found his bank failed to demonstrate Boyd had been negligent.

When scammers trick you into passing on stolen money

Another scam is to ask people to accept and forward money stolen from another victim's bank account. In this way, they become what is known as a "mule". Scammers convince people there is a legitimate reason for the transfer, such as paying a fee associated with a job application or refunding an accidental overpayment from an online purchase.

If this happens to you and the money is found to have been stolen, a bank may reverse the payment into your account, causing your account to be overdrawn if there isn't enough money in it. The bank will ask you to repay the overdrawn sum.

In such cases, we consider whether the bank's terms and conditions allow it to reverse a payment from your account. We also assess whether the bank had sufficient information to conclude the money was stolen before it reversed the payment. If so, you will be held liable for the loss.

Additional resources

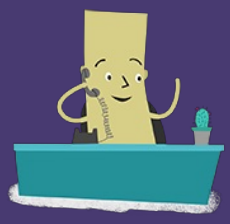
https://www.consumerprotection.govt.nz/scams/scam-alerts

https://www.netsafe.org.nz/

https://www.fma.govt.nz/investors/scams/

https://www.cert.govt.nz/

https://www.police.govt.nz/advice/email-and-internet-safety/internet-scams-spam-and-fraud



Never give out your PIN or internet password, your bank will never ask for them. Use our tips above to double-check who you are dealing with.