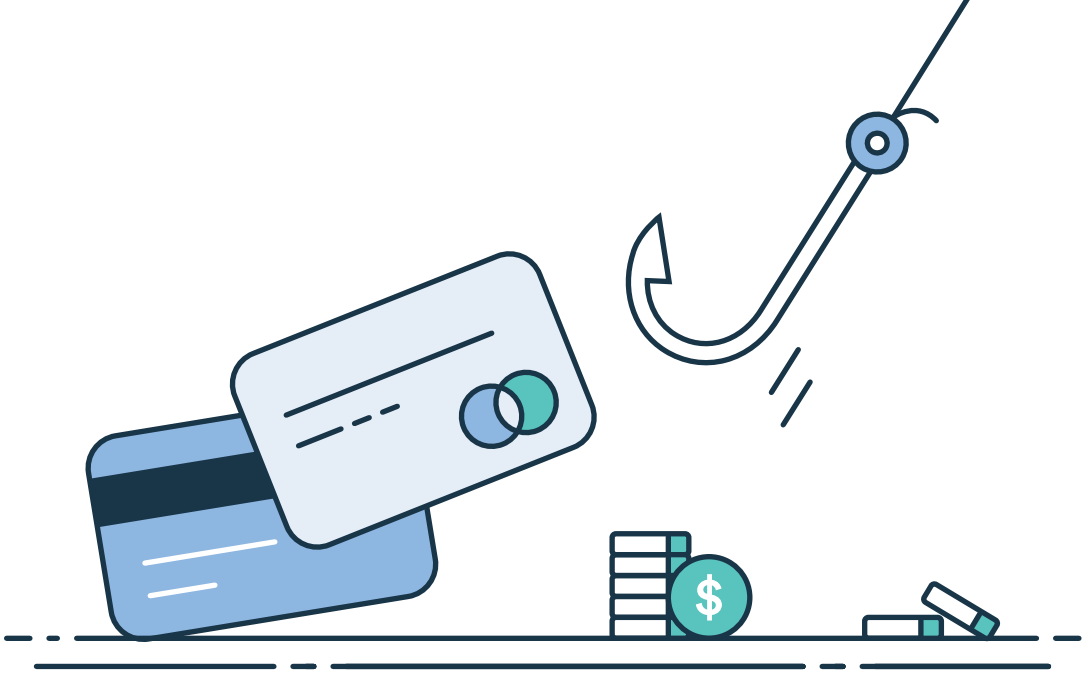
How to keep yourself safe from online scams



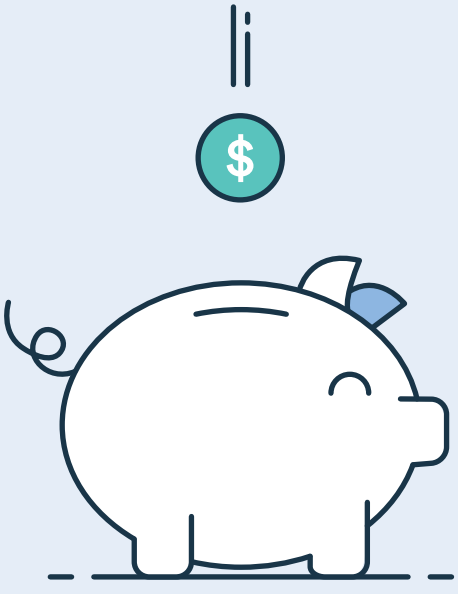
How do scams work?

Fraudsters are always looking for new ways to scam us and steal our money. They use a range of ways to trick people into handing over personal information.

Once they have your bank account number, log in details, or password, they can access your identity and your money.

Personal information includes your date of birth, address, driver's licence and passport details, and bank statements. Anyone who asks for these will likely be trying to scam you.

Fraudsters may pretend to be your bank, a government agency, a retailer or someone you trust.



Reimbursement for losses

Depending on what happened, your bank may be able to reimburse you for any money taken from your account.

You must still protect access to your bank accounts. If you give anyone else account access, you may be liable for the loss.

How is my bank helping to keep me safe?

Customer security is a major priority for all banks. They work hard to protect you from financial crime.

Your bank has a range of security measures to help protect your personal account information.

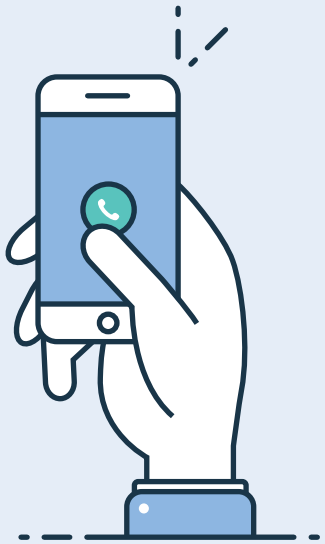
If your bank suspects fraudulent activity they will contact you and can temporarily freeze your internet banking to prevent further fraudulent transactions.

Even then, they will never ask for your log in details or password.

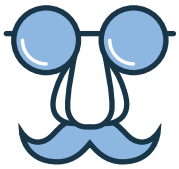
What should I do if I think I have been scammed?

If you think you've been the victim of a banking scam, contact your bank immediately.

You should also change your internet banking password as soon as possible.



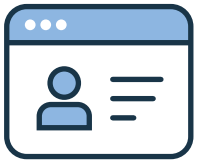
How can I protect myself from scams?



Check who's emailing you is legitimate. Fraudsters may disguise their identity.

Beware of emails from people or companies that you do not know.

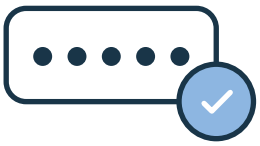
Do not click on links in any suspicious looking emails, or reply to them.



Only give your personal information to people & organisations you trust.

Type in the address for internet banking. Avoid clicking on email links.

Only bank on secure websites with the padlock symbol in the address bar.



Don't share your login details or password with anyone.

Avoid public computers & WiFi for internet banking e.g. cafés, libraries etc.

Keep your computer's security software up to date.

Where can I find more information?

Ask your bank for more information, or visit these websites:

www.scamwatch.govt.nz
www.netsafe.org.nz
www.cert.govt.nz
www.police.govt.nz
www.ageconcern.org.nz

NEW ZEALAND BANKERS ASSOCIATION