



## PREVENTING FRAUD AND SCAMS

As our world becomes increasingly connected digitally, it's more important than ever that we stay aware of potential threats to our safety in the technology space.

### Staying Safe Online

- Never give out your passwords, log in details, or account info.
- Don't respond or click on any links to verify your account information, even if it looks like it's from a real organisation.
- Never share personal or financial information by text or email.
- Do not respond to texts from unknown numbers, or any that appear suspicious.
- If a 'friend' sends you a text with a suspicious link, call them to make sure they weren't hacked.
- If a business or organisation sends you a text that you weren't expecting, call them to verify its authenticity using the phone number on your bill or statement (or their official website).
- If you receive an email from a business or organisation and suspect it might not be from who it claims, look carefully at the email address and cross reference it to those provided on the official website. If still not sure, call the phone number listed on the official website to clarify that the email was truly sent from the organisation.
- Only shop on trusted and verified websites. Look for the padlock icon by the website address.
- Be wary of unexpected deals, contests, or log in requests.
- Check and adjust your privacy settings.
- Log out after using a shared computer.
- Report suspected scams.

If you receive suspected spam content you can report it to the Department of Internal Affairs:

- Report email spam by forwarding to [complaint@spam.govt.nz](mailto:complaint@spam.govt.nz) (use if email has attachments)
- Report email spam by using an [online form](#) (don't use if email has attachments)
- Report text spam for free on your phone by forwarding the spam text message to **7726**.

You can also contact Netsafe for help with the steps to take should you fall victim to a scam or cyber bullying by submitting a report on [netsafe.org.nz](https://www.netsafe.org.nz) or by calling **0508 NETSAFE** or emailing [help@netsafe.org.nz](mailto:help@netsafe.org.nz). They also have lots of useful resources and advice on their [website](#).



## PREVENTING FRAUD AND SCAMS

### Credit Card and Eftpos Fraud

Theft of credit and EFTPOS cards is a common crime in New Zealand. So too is the associated fraud that comes with someone using a stolen card to purchase goods or services.

While Police work closely with banks and retailers to prevent this type of fraud, there are a number of simple things you can do to assist.

- Keep your credit or EFTPOS card safe. If it is stolen or goes missing, inform your bank or credit card company right away and have it canceled immediately.
- Guard your Personal Identification Numbers (PIN) closely. Never give it out to anyone and avoid any easily guessed codes such as your date of birth or sequential numbers i.e. 1234.
- Never keep your PIN and card in the same place. Memorise it and ideally use different PINs for different cards/accounts.
- Destroy expired cards and sign new cards immediately.
- Match credit card and bank statements with your receipts. Follow up on any discrepancies.
- Keep a secure record of your card number, expiry date, and any numbers to call if your card is lost or stolen.
- Tell your bank or credit card company if you change your address so replacement cards are sent to the correct place.
- Look out for tampering of ATMs, EFTPOS machines and fuel pumps. Obvious signs of tampering include anything loose, crooked or damaged. Avoid using a machine if anything looks unusual. Use machines in well-lit, visible sites and cover the keypad when entering your PIN.
- Know who you're dealing with when shopping online. If you're unsure, do a background check to make sure other's haven't reported the website as a scam. If the deal sounds too good to be true, it probably is!
- Only make telephone transactions when you have instigated the call and are familiar with the company or individual. If in doubt, get them to send you an email with more information you can verify. Never feel pressured to provide sensitive information or pay right away.

**If dealing with customers, be wary of anyone who:**

- Is nervous, trying to hurry things up or is using a newly valid card.
- Looks at the card before signing the transaction slip or signs slowly and awkwardly.
- Has a large number of cards and attempts to use several before one is approved.
- Watches closely during the authorisation request or can't provide photo ID.
- Purchases an unusual amount of expensive or random items indiscriminately.