GET SET UP FOR SAFETY

Common Types of Scams

There are hundreds of different stories scammers use to try and trick you, but almost all scams are centred on a fake situation, fake person/ organisation, fake product or fake service, and often a combination of these factors. For example:

Phishing Scams

Scammers often impersonate trusted organisations like banks or Scammers impersonate trusted organisations to steal your credentials, personal data, and money.

SIGNS: Urgent requests to log in or provide verification information, links or phone numbers to click, fines or payments to be made.

ACTION: Don't click on links or download attachments. Verify the request by contacting the organisation directly.

SPONSORED BY
CHORUS | netsafe

Shopping Scams

Fake online stores or marketplace scams where items are never delivered or not as described.

SIGNS: Unrealistic prices or sellers demanding quick, untraceable payments like gift cards.

ACTION: Use secure, reputable sites and payment methods. Check reviews and profiles for legitimacy.

Romance Scams

Romance scams involve scammers building a fake online relationship to gain trust and steal money or personal information.

SIGNS: Fast-moving relationships, avoiding meetings, requests for money, emotional manipulation.

ACTION: Be cautious about sharing personal information. Verify the person's identity and do not comply with requests for money.

Investment Scams

Scammers offer fake investment opportunities, often endorsed by celebrities, to steal money.

SIGNS: Unexpected calls about investment opportunities, promises of very high returns with little risk, or asked to keep the investment a secret.

ACTION: Investigate before investing, check the company's legitimacy, and verify with the Financial Markets Authority

Identity Theft

Scammers can steal your personal information to commit fraud, such as making purchases or applying for loans, pretending to be you.

SIGNS: Requests for personal information, unsolicited emails or messages, and suspicious activity on accounts.

ACTION: Protect personal information and be careful what you share, use strong passwords, and update security software regularly.

Emergency Scams

Scammers impersonate family members in distress to trick victims into sending money.

SIGNS: Urgent requests for money, claims of accidents or arrests, and new phone numbers.

ACTION: Verify the story by contacting the family member directly and never send money to unknown individuals. Agree on a secret word: Encourage whānau and friends to decide on a private phrase that can quickly confirm a caller's identity.

Health & Medical Scams

Scammers offer fake health products or miracle cures.

SIGNS: Unbelievable claims, celebrity endorsements, and requests for advance payments.

ACTION: Consult healthcare professionals and verify the legitimacy of online pharmacies.

Subscription Traps

Scammers offer free trials that lead to expensive subscriptions.

SIGNS: High-pressure sales tactics, unclear terms and conditions, and frequent charges.

ACTION: Research the company, read reviews, and monitor credit card statements.

Tech Support Scams

Scammers pretend to be tech support to access your device or charge for fake services.

SIGNS: Pop-ups or calls about viruses, remote access requests, or payment demands.

ACTION: Never grant remote access. Contact your provider using verified details. Avoid paying for unsolicited support.

Account Compromise

Scammers hack accounts to steal information, send scams, or make unauthorised transactions.

SIGNS: Unusual account activity, unexpected logins, or messages you didn't send.

ACTION: Use strong, unique passwords and enable 2-factor authentication. If compromised, change passwords and report it immediately.

Spot the Red Flags and Take Action with SCAMS

S **SURPRISE:** Be cautious of unexpected messages or calls, especially if they claim to be from official organisations like banks or utility companies.

C **CONTROL:** Scammers may rush you to make a quick decision or move to a different online space. They might say you'll miss out on a prize or be penalised if you don't act immediately.

A **ACCESS:** Be wary if asked to share passwords or personal information. Scammers might ask you to verify your account, correct an error, or give remote access to fix a problem.

M **MONEY:** Be suspicious if asked to pay online for something. Scammers might ask for a processing fee, gift cards, cryptocurrency or credit card details.

S **STOP COMMUNICATING AND SEEK SUPPORT:** Don't click on links, give information, or send money. Hang up the phone if they've called you. Contact your bank and the police if you've paid any money.

Get Set Up for Safety

Find more on Netsafe's scams webpages or download our Little Black Book of Scams, and explore Netsafe's free Get Set Up for Safety resources for tips on online safety, from scams to information security.

Find out more netsafe.org.nz/olderpeople