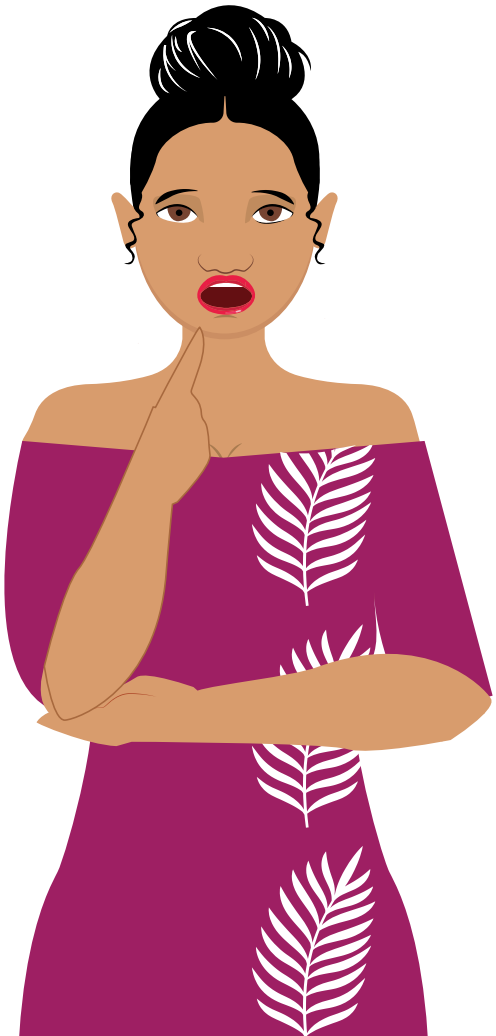
Spotting and Avoiding Online Scams



Going online to connect with other people can be fun and rewarding. But it's important to be aware that not all connections or people are what or who they seem. Scammers can be very clever and may target anyone, and try to trick you or someone you know out of money or personal information. It's important to learn how to identify and avoid scams so that we can help to protect ourselves and our friends and family.

Common types of scams

Scams can happen in different ways, including through email, social media, phone calls, text messages and even traditional letters or other documents. Common types of scams include:

- **Prizes and promotion scammers** may claim that you've won a prize or lottery and ask you to pay or share your personal information to receive it - but in fact, there is no such prize.
- **Friendship scammers** may flatter you and tell you that you look 'beautiful' or 'interesting', or claim to be very rich. They may try to become your friend, but then later cheat you into giving them money, or sharing your personal information or private photographs.
- **Charity scammers** may pretend to be an organisation or person that's collecting donations to assist a person or people in need. But it turns out they are simply trying to get this money for themselves.
- **Job, loan, investment and cryptocurrency scammers** may offer a great job, cheap loan or other way to make quick money and ask for payment to access the opportunity, but actually this does not exist.
- **Phishing** is when a scammer tricks people by pretending to be a real shop, bank or organisation, into sharing personal information like their name, address, bank details or online passwords. They might then use this information to pretend to be you, to cheat other people out of money or information.

Scammers sometimes also create fake messages that look like they're from Facebook. Facebook will never ask you for your password in an email, or send you a password as an attachment. Learn more.

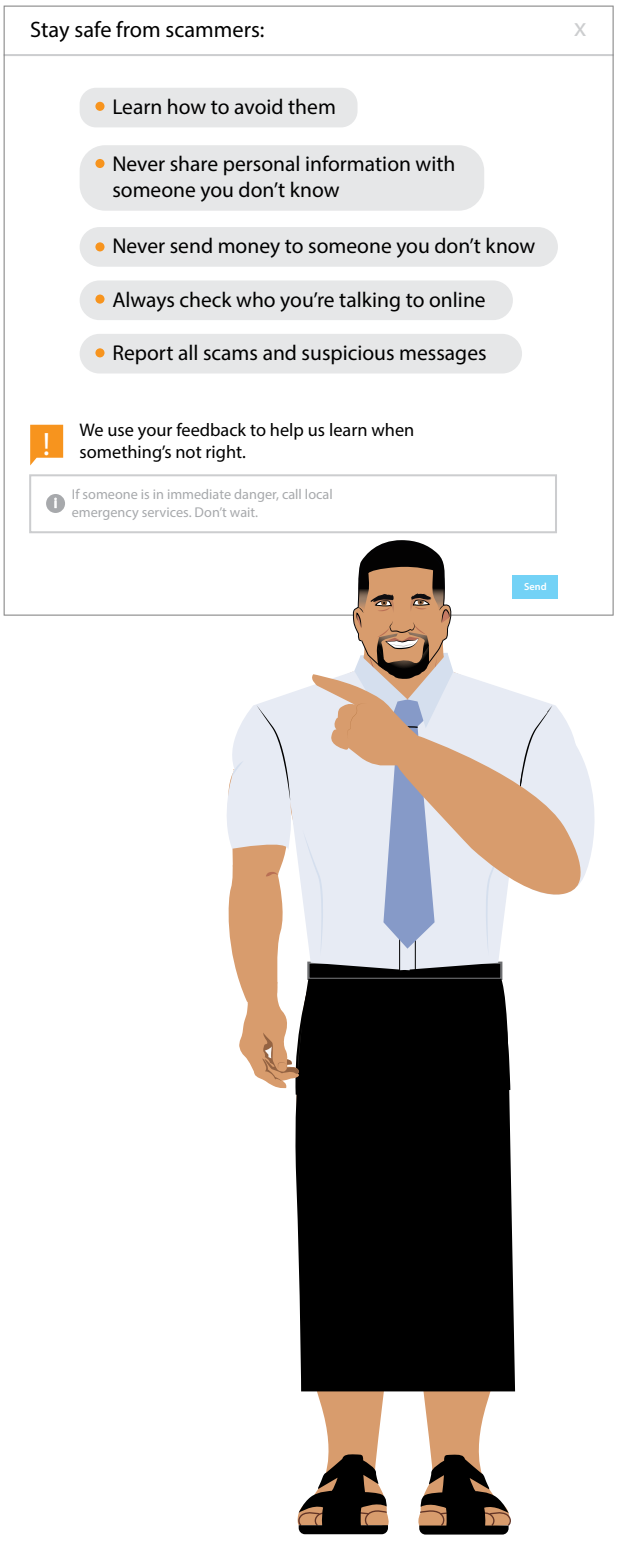
How to spot a scam

Be wary of the following - they may be a sign that something is a scam:

- A message asking you to confirm your personal information, such as your name, address, date of birth or bank account details.
- A claim there is a problem with your bank account or payment information.
- Anyone asking you to pay them a fee.
- Messages with a threat or sense of urgency.
- Messages with poor spelling and grammatical mistakes.

Remember - if something seems too good to be true...it probably is.

Spotting and Avoiding Online Scams cont.



How to avoid scams

- If you ever feel unsure about a message you've received, don't open it, and don't respond to the person.
- Always be careful if you receive a message from someone you don't know.
- Never pay money to, or share your - or anyone else's - personal information with someone you don't know. Personal information includes people's names, age, phone number, email or home address, school, or photo identification (like a passport or driver's licence).
- Remember that scammers may even pretend to be someone you know, like a friend or family member. If you suspect this may be happening, you can contact that person another way to make sure it's them, for example using the phone number you know to be really theirs.
- Always research who you're dealing with - visit the organisation's official website or call their phone number to confirm they are who they say they are.

Report all scams or suspicious messages immediately. Find out more about reporting scams on Facebook and Messenger, Instagram and WhatsApp.

If you think you may have been scammed

- If you gave a scammer your online account information (login, password etc.), change your password right away. Create new passwords that are strong and unique.
- If you use the same password for multiple accounts or websites, change them all.
- If you have paid a scammer with a credit or debit card, contact your bank or credit card company right away. Report the scam and ask what steps you may be able to take to reverse the charges.

If you or someone you know is the victim of a crime or is in immediate danger, contact your local law enforcement or police for help.

For more information, see Netsafe New Zealand's Tips to Avoid Scams.