

BEWARE OF SCAMS AND

Stay Safe Online



- Never give out your passwords, log in details, or account info.
- Log out after using a shared computer.
- Don't click on links to verify your account information.
- 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 an 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).



Creating safe, resilient, and connected communities.

- If you receive an email from a business or organisation and suspect it might not be from who it claims, look at the email address and cross reference to those on the official website. If not sure, call the phone number listed on the official website.
- Only shop on trusted 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, or ask someone to help you.
- Report suspected scams to the Department of Internal Affairs:
 - Report emails by forwarding to complaint@spam.govt.nz.
 - Report text for free on your phone by forwarding the text to **7726**.

**In an emergency call 111 or to contact the
POLICE call 105.**

**FOR MORE TIPS & ADVICE JOIN
NEIGHBOURHOOD SUPPORT TODAY**

neighbourhoodsupport.co.nz

0800 4 NEIGHBOURS



Creating safe, resilient, and connected communities.