Soilleir

Stay Safe Online

A quick guide to keep beside your phone or computer. You don't have to be a technology expert.

1. You are in control

You don't have to answer an unexpected call, reply to a message or click a link. If you're unsure, stop. Contact the person or organisation yourself using a number or website you already trust.

2. Look out for pressure

Be careful if someone demands money, passwords or security codes, says you must act immediately, or tells you to keep the conversation secret. A friendly voice or familiar logo is not proof that a request is genuine.

3. If something has already happened, act promptly

Don't panic, but don't put it off. These situations need attention:

▲ You shared a password: Change it using the real website or app. Change it on other accounts if you used it there too.

▲ You shared banking details or sent money: Contact your bank immediately using its official app or a number you know is genuine.

▲ You installed something or allowed device access: Stop using that device for banking. Disconnect it from the internet if someone may still be controlling it, and get trusted technical help.

▲ Someone got into your account: Use the account provider's official website or app to secure or recover it. Ask someone you trust to help.

4. Ask for help

Tell a family member, friend or someone you trust. There is no shame in asking. If money is involved, call your bank first. For New Zealand cyber incident advice and reporting, visit ncsc.govt.nz. For online safety support, visit netsafe.org.nz. In immediate danger, call 111.

5. Small habits help

Use different passwords for important accounts. Keep passwords and sign-in codes private. Turn on two-step verification if available (an extra check when signing in). Keep your phone, computer and apps updated.

Remember: Before you act, you can stop and check. If you've already shared money, sensitive information or device access, act promptly and ask for help.