What are the risks?

If you or your family use the internet, there are risks you need to be aware of.

Online viruses travel like a sickness through the internet and can destroy your devices or steal money.

Phishing scams look and sound like real websites, emails, texts and calls, to trick you into giving over money or personal information, or downloading a virus.

Scammers might pretend to be your friend or someone who cares about you to steal from you.

With your information, people can pretend to be you for fraud and other crime.

PaCSON
PACIFIC CYBER SECURITY OPERATIONAL NETWORK

CUP CYBER UPSKILL PROGRAM

We're all in this together

If you're unsure about anything online, talk to your friends, family and community. The more we talk about cyber safety, the safer we all are.

Scams and viruses can happen to anyone.

If you think you have been scammed, stop all communication with the scammer and contact the police.

Ask the person who gave you this flyer about more resources, including tips for parents and more about staying safe from scams.

How to be cyber safe

Protect yourself and your community

If you use the internet on any device – like a phone, computer, tablet, gaming platform, or something else – you need to know how to use them safely.

Online criminals are always looking for new ways to steal money and personal informational. Follow this guide to stay one step ahead, to help protect yourself, your family and your community.

How to be cyber safe

- Use a different strong and secret password for every device and account you have.
- Always know where your devices are.
- If you share a device, always log out of your accounts, like social media and emails.
- Turn on automatic updates for your apps and devices.
- Back up your devices – keep a copy of your photos, contacts and documents.
- Never click on funny-looking links or reply to strangers.
- If you can, avoid free public Wi-Fi, especially for shopping or banking.
- Only download from trusted sources, such as your phone's official app store.
- Don't post or share any personal information online, like where you live or work, your phone number, or financial details.
- Make your social media accounts private so only your friends can contact you.

Be aware of scams

If something seems fishy, it probably is!

Signs it's a scam:

- Bad spelling or mistakes, including in email addresses, links and names.
- Greetings like "hello dear", "dear customer" or "hi friend".
- Claims to be someone official, like the bank or police.
- Promises of – or requests for – money.
- Someone asking you for private information or an urgent favour.
- Someone asking you to click on a link or download something.
- The message just seems weird – very formal, confusing, demanding, threatening or not in your local dialect.

Never give away money or personal information, open messages or downloads from people you don't know, or click on weird links and pop-ups.

If you're not sure, just don't click!

Password protect it!

With your password, a scammer can get your personal information and could steal your money or pretend to be you.

A password is like your toothbrush. It's yours and you shouldn't share it with anyone else. That means making it difficult to guess.

Top password tips

- Use upper and lowercase letters, numbers and symbols.
- Try a mix of four or more random words.
- Don't use something obvious like your birthday, username or your pet's name.
- Use a different password for every account.
- Never tell anyone your password.
- If you can, turn on two-factor authentication.