National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

Keeping safe online

Why is cyber security important for me?

The internet and social media are amazing platforms that help us share information and stay in touch with friends and family.

However, criminals and other unlawful organisations also use them to try to get your money, your information or to intimidate you.

They can operate from anywhere in the world, speak most languages fluently and create convincing fake websites. They will contact you via email, social media and text message and they will try to make you feel scared or anxious, so you aren't thinking clearly.

All of this means you need to be prepared and always aware of the tricks they use.

What are some common issues I may come across online?

These are some of the most common situations we see.

- You get a suspicious email or text message asking you to click a link.
    - These links often lead to fake websites that are designed to steal your login or financial details.
- You get a suspicious call that asks for personal information.
    - As above the caller will pretend to be from your bank and ask for information.
- You receive communication from someone pretending to be a person of authority, trying to get you to do something.
    - Often the person makes some kind of threat.
- Someone gets into one or more of your online accounts (for example: email or social media).
    - If someone gets into your online account they could steal information, redirect payments, and potentially target your friends or family by pretending to be you.
- Your credit card details are stolen, or you are scammed out of money in a fake sale or investment.
    - Scammers are hoping you will see a good deal and want to pay without thinking. Or perhaps a real website is caught in a data breach and your details are leaked online.

There are more scenarios here:
Get help now - Own Your Online

How do I stay secure online?

- **Long and unique passwords.**
    - The longer a password is, the stronger it is.
    - Create a memorable password of more than 16 characters by joining four random words together (for example: TriangleRhinoOperationShoes) and adding in numbers, capital letters and symbols if required (for example: Triangle&"Rhino"Operation2Shoes).
    - Importantly, do not repeat your passwords. If a criminal gets one of your passwords they will try it on other accounts as well.

    - Use a password manager to remember your passwords for you and to create new passwords.
    - Create good passwords - Own Your Online
- **Have two-factor authentication turned on.**
    - This is an extra piece of information – usually a code on your phone – that you need to log into a website.
    - This technique is incredibly strong and can stop most attempts to get into your accounts.
    - We recommend using an 'authenticator app', where this is supported.
    - Set up two-factor authentication (2FA) - Own Your Online
- **Stay private online.**
    - The best option to stay secure on social media is to have your privacy settings turned on.
    - This will stop random people, including cybercriminals, being able to see your posts or sending you messages.
    - Still be careful posting personal information about yourself, your family or your friends.
    - Make sure contacts are who they claim to be.
    - Watch out for fake friend requests. Be careful of people claiming to be journalists or others you don't know well.
    - Protect your privacy online - Own Your Online
- **Keep everything updated.**
    - When you update your phone, computer or software, it plugs any holes there may be in the security as well.
    - The criminals are always looking for ways to get in and updates fix the vulnerabilities.
    - Restart your devices regularly.
    - Keep up with your updates - Own Your Online
- **Be aware of scams.**
    - The best advice is to be aware of these scams and look out for them.
    - If anything seems wrong, do not engage with the person who contacted you. Especially be cautious if they ask for money, even if they seem friendly.
    - Look for strange links and email addresses (for example: your bank will not send you an email from a Gmail account).
    - *Never* click links in text messages.
    - Only download apps to your device from official app stores.
    - If in doubt, contact the organisation that contacted you directly and do not follow any links or phone numbers you get sent.
    - Try to stay aware of online security risks for yourself, your community, and any groups you belong to.
- **Protect your information.**
    - Use encrypted messaging apps, such as Signal. This will stop anyone from being able to read your messages.
    - Only share information with a website if the address starts with HTTPS. The S stands for "secure" and means any information sent between you and the website is encrypted.
    - Consider using a virtual private network (VPN) which can protect your data and hide your location.

    - Check what data and permissions your apps have access to. For example, a fitness app doesn't need access to your contacts.

What do I do if I get scammed or worse?

There are a lot of places you can go to for help. These organisations will not share your details with anyone else, unless you give your consent.

- You can report cyber incidents to the NCSC through the CERT NZ portal and we can help or put you in touch with another agency:
  Report an incident | CERT NZ
- If you have lost money, you should contact your bank immediately.
- Scam text messages can be forwarded, free of charge, to 7726, a service run by the Department of Internal Affairs.