certnz

Te Kāwanatanga o Aotearoa
New Zealand Government

Keeping safe online:

cyber safety tips

Published: May 2022

What you will find in here

What this document is about 2

Having a secure password 6

Keeping your passwords safe..... 9

Using 2 steps for extra security 13

Updating your device 15

Being careful about the information you share 17

Telling someone about a cyber attack 19

What this document is about

CERT NZ has written this document about **cyber security**.

CERT NZ:

- is a government agency in New Zealand
- works to keep us safe from **cyber security threats**.

Cyber security is about keeping ourselves safe online when we use **electronic devices.**

Electronic devices are things like:

- cell phones / mobile phones
- computers
- tablets.

A **cyber security threat** is when someone wants to:

- steal your **private information**
- stop you getting your online information.

People who make cyber security threats are called **cyber attackers**.

Private information is also known as personal information.

Private information tells someone your:

- name
- other information about you such as your bank account number.

Cyber attackers are people who steal your private online information.

Cyber attackers work online so you will not be able to see them.

Cyber attackers might try to steal your:

- bank account number to take your money
- name so they can pretend to be someone else

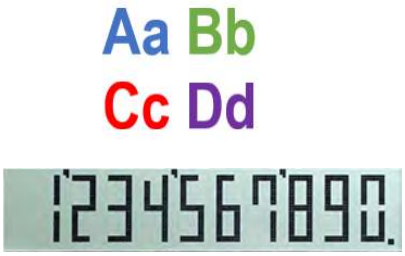
- social media accounts like Facebook so that you cannot use them.

A cyber attacker might also send you links to other websites.

Sometimes clicking on these links can mean your electronic device gets a **virus**.

A **virus** means you may not be use your computer or device.

Having a secure password



A **password** is a group of characters like:

- letters
- numbers
- symbols on your keyboard like $.

You are the only person that knows your password.

Passwords keep online information about you safe.

Using your password shows you are the right person to see your information.

Passwords need to be **strong**.

A strong password means it is hard for someone to guess.

Strong passwords:

- are long
- are unique meaning they are different from anything else
- do not use personal information like your birthday.

To make it easy to remember a strong password use:

- a sentence of about 4 words

and

- a number

and

- a symbol like $ or & or !

For example:

- **popcornwithbutteryum!1**
- **Birdsaresingingloud&5**

Keeping your passwords safe

You need to use a different password for each of your **online accounts**.

An **online account** is a place you go on a website to use a service like:

- a bank where you put in and take out money
- an online shop where you buy things
- a government agency you get support from.

Each service uses an **application or app** to manage its services.

An **application or app** is a program on your electronic device that lets you do things like:

- banking
- shopping
- social media like Facebook or TikTok.

You will have an account with a password for each service you use.

The service keeps information about you online like:

- your address
- your phone number

- your bank account.

You may have a lot of passwords to remember.

You can use a **password manager** to:

- keep your passwords safe
- help you remember them.

A **password manager:**

- stores all your passwords in one place online
- is like an online safe.

You use 1 very strong password for your password manager.

The password manager will then put in the right password for each site or app.

Using 2 steps for extra security

You can keep your online information safe by doing something called **two-factor authentication**.

Authentication means to show that something is true.

Two-factor authentication uses 2 steps to keep your information safer.

Two-factor authentication is also known as 2FA.

2FA means you use 2 steps to:

- get your online information
- keep your online information safe.

Most of the time 2FA works by:

- Step 1 – entering your password

- Step 2 – entering a code sent to your phone or email.

2FA can also be turned on in the privacy settings of your:

- phone
- tablet

- applications / apps
- accounts.

Updating your device

Sometimes you will get an **update** message on your electronic device.

An **update** is when changes are made to applications / apps to:

- make them more secure
- stop cyber attackers from getting your information.

Your device will tell you when there is an update.

Install the update as soon as possible.

Install means adding the update to your device.

You can set your device to **automatically install updates** so you will not miss one.

Automatically install updates means that you agree to letting the update change the application / app.

Being careful about the information you share

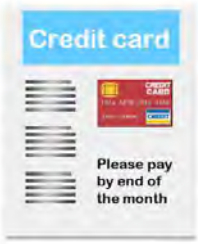
Cyber attackers could use information you share online to:

- access information about you
- **steal your identity**.

Steal your identity means that someone pretends to be you

They use your information to get:

- money from your bank account
- credit cards in your name which you have to pay for.



To keep your personal information safe:

- be careful how much personal information you share online

- know who you are sharing personal information with

- think about why a person or business might want information

- do not give anyone information if you are not sure.

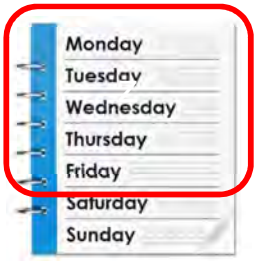
Telling someone about a cyber attack

You can talk to CERT NZ to tell them about a cyber attack.

You can phone them:

0800 237 869

It will not cost you any money to call this number.



CERT NZ is open:

- Monday to Friday

- 7am in the morning to 7pm in the evening.

This information has been written by CERT NZ.

It has been translated into Easy Read with advice from the Make It Easy service of People First New Zealand Inc. Ngā Tāngata Tuatahi.

The ideas in this document are not the ideas of People First New Zealand Inc. Ngā Tāngata Tuatahi.

Make It Easy uses images from:

- Changepeople.org
- Photosymbols.com
- SGC Image Works
- Huriana Kopeke-Te Aho.

All images used in this Easy Read document are subject to copyright rules and cannot be used without permission.