NCSC

own your online

Easy Read

5 quick steps to online security

Published: May 2026

About this Easy Read

This Easy Read is by the **National Cyber Security Centre**.

The **National Cyber Security Centre**:

- is a government agency
- works to keep everyone secure when using the internet.

In this Easy Read the National Cyber Security Centre will be called the **NCSC** for short.

Where you see **we / us** this means the NCSC.

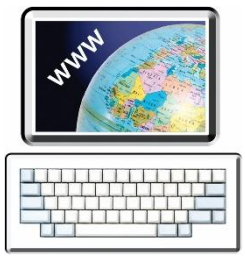
This Easy Read is about 5 easy ways you can be **secure** online.

Here **secure** means doing things online that will stop people stealing your:

- details / information
- money
- accounts.

own your online

You can find more information about online security at the Own Your Online **website**:



www.ownyouronline.govt.nz/alt

Why is being secure online important?

People do a lot of things online like:

- meetings
- interviews

- banking
- buying tickets.

This:

- makes our lives easier

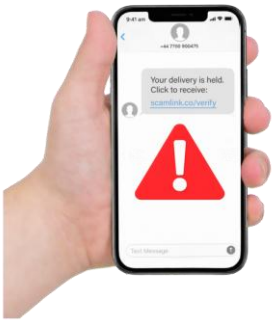
but

- means that our information is not always secure.

The NCSC is getting a lot more reports about online security problems.

Attackers are making **scams** to:

- steal credit card information
- get into:
    - bank accounts
    - emails
    - **social media** accounts.



Here **scam** means tricking someone into giving out their details / information.

Social media is things like:

- Facebook
- TikTok
- Bluesky.

Getting caught by a scam could:

- lose you money
- make you feel upset.

You can do things to stop online security problems from happening.

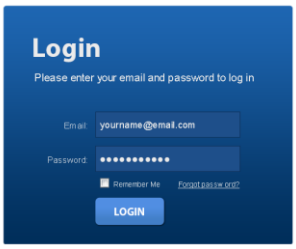
A few small changes to your online security will make a big difference.

The 5 easy steps

1. Make strong passwords

A simple security change you can do is make a password that is:

- long
- strong
- unique / different to other passwords you use.



Sometimes the same password is used for many different accounts.

This means an attacker can get into other accounts if they have that password.

What can I do?

Try making a **passphrase** instead of a password.

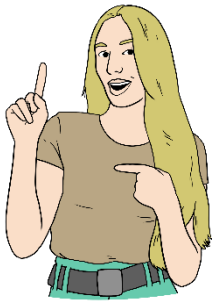
A **passphrase** is a set of 4 or more words.

A passphrase is often:

- easier for you to remember

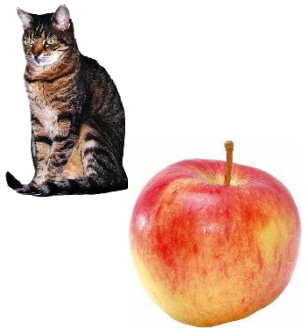
but

- hard for attackers to figure out.



You can try making a passphrase that is:

- fun
- means something only to you.



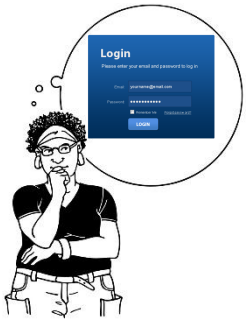
Examples of passphrases are:

- catseatredapples
- grapewineisfruitsalad.

Do not use passphrases of words that are easy to find like:

- family names
- birth dates
- addresses.

You could use a **password manager** to store your passwords if you are worried about remembering them.



A **password manager:**

- stores your passwords
- protects your passwords
- creates secure passwords for you.

Having a password manager means you only need to remember the login details for 1 thing.

2. Use two-factor authentication / 2FA

Two-factor authentication / 2FA is a code which is sent to you to show it is really you trying to get into your account.

A two-factor authentication / 2FA code can be sent to your:

- phone
- computer
- tablet.

Two-factor authentication / 2FA is a good way to keep attackers out of your accounts.

What to do

Turn on two-factor authentication / 2FA for your important accounts like:

- online banking
- email
- social media.

You can usually find this in the settings section of your accounts.

Using two-factor authentication / 2FA by text is much safer than not using it.

We think it is better to use a different way to get two-factor authentication / 2FA like an **authentication app**.

Here an **authentication app** is an app that will send you a code for two-factor authentication / 2FA.

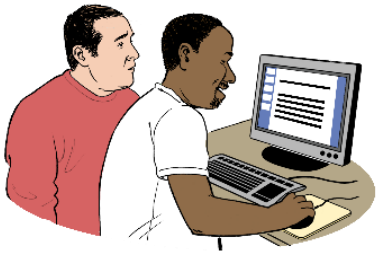
An authentication app can go on your:

- phone
- tablet.

3. Turn on automated updates

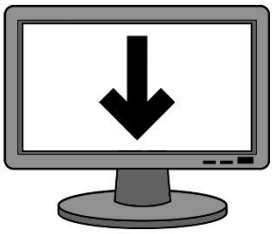
Automated updates protect you from problems that might let attackers into your devices by doing updates to:

- devices like your computer
- apps.



People who make computer software can:

- quickly fix a problem when it is found
- send the software update to your device.

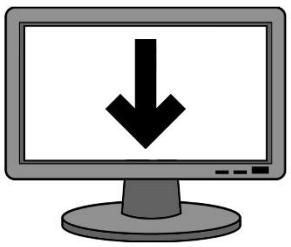


It is important to do updates straight away when they are available.

What to do

Set **automatic** updates to happen on your:

- devices like your computer
- apps.



Here **automatic** means something happens without you doing anything.

The easiest way to do this is:

- go into settings

  and

- turn on automatic updates.

4. Make social media private

You can turn your social media privacy settings to:

- private

or

- friends only.

This lets you control who:

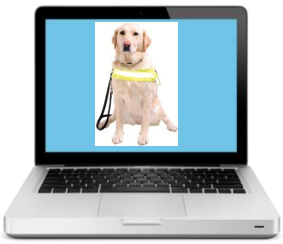
- sees the information you share
- you share information with.

This protects everyone from scams.

What to do

Do not put too much information about yourself on your social media accounts.

Remember to be careful about your passwords.



For example you might share a picture of your dog on Facebook.

Do not make your password the name of your dog.

5. Think before you click

Be careful about opening:

- links
- attachments.

They could be:

- in text messages

- in emails
- on social media.

Attackers can use them to:

- get your information
- put software on your device that could harm it.

It is better to be careful even if you think the link is okay to use.

What to do

Check before you give out your information.

Make sure you know:

- how the companies you deal with will contact you
- what kind of information companies will ask for.

For example a bank will never ask you to login by sending you links to online banking.

Call the company direct if you are not sure why you are being asked for information.

The law says businesses must only ask you for information they need.

Another example is you might get a message online from someone you know asking for:

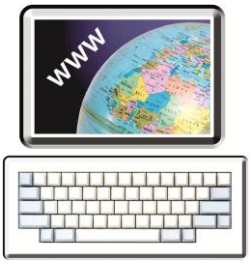
- money
- help.

Find out if it really is them by contacting them another way.

Report an incident

The NCSC can support you if you have:

- had a security problem online
- been targeted by a scammer.



You can make a report online at this website:

www.ncsc.govt.nz/report-issue

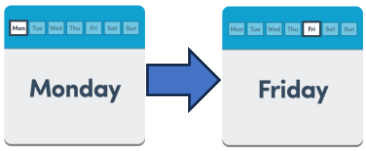
This website is **not** in Easy Read.

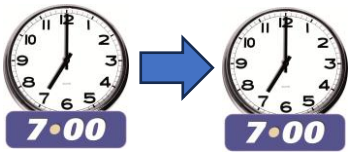
You can phone us if you need support making your report.

You can **phone** us on:

0800 114 115

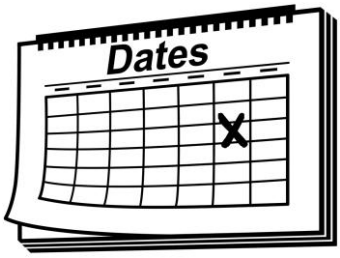
This number does not cost money to call.





You can phone us from:

- Monday to Friday
- 7 am to 7pm.



We are not open on **public holidays**.

Public holidays are days like:

- New Years Day
- Good Friday
- Christmas Day.

If you find it hard to use the phone the **New Zealand Relay** service is for people who are:

- Deaf / hard of hearing
- deafblind
- speech impaired / find it hard to talk.

You can find out more about the New Zealand Relay service at:

www.nzrelay.co.nz

This Own your Online information has been written by the National Cyber Security Centre.

It has been translated into Easy Read by the Make it Easy Kia Māmā Mai service of People First New Zealand Ngā Tāngata Tuatahi.

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

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

Make it Easy uses images from:

- Photosymbols
- Change Images
- Huriana Kopeke-Te Aho
- SGC Image Works
- T Wood
- Studio Rebeko
- Inga Kramer.