NCSC

own your online

Easy Read

Keeping safe after a data breach

Published: May 2026

About this Easy Read

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

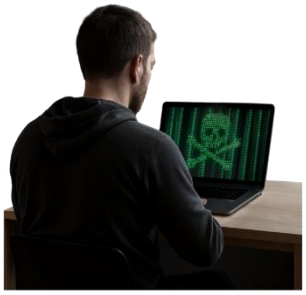
The **National Cyber Security Centre**:

- 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 keeping safe after a **data breach**.



Here a **data breach** is when your private information held by a business can be seen by anyone.

This usually happens by accident.

own your online

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

www.ownyouronline.govt.nz/alt

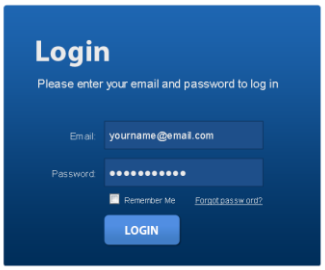
Why does a data breach matter?

A data breach is when your personal information held by a business is made public / seen by other people by accident.

This can include your:

- name
- email address
- username

- records to do with money like your credit card



- login details.

Some data breaches might just put out your email address.

Other data breaches might put out more important details like your:

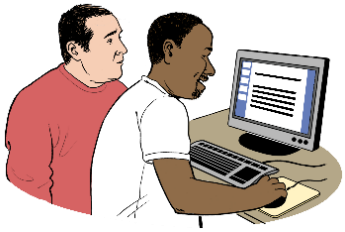
- passwords
- passport details
- banking information
- identification / ID.

It is very important to take steps when there is a data breach so:

- there is not much damage done like losing money

- your personal information is protected.

How to protect yourself after a data breach



1. Confirm the breach

Find out if your data has been leaked.

You might hear about the data breach from the organisation it happened to.

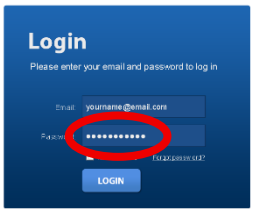
Contact the organisation if they have not told you what is going on.

This will support you to know what information has been leaked.

2. Change your passwords

Change the passwords straight away on:

- the accounts that have been breached
- your most important accounts like:
    - email
    - banking.



Use 1 password for only 1 account.

This means an attacker will not be able to get to your other accounts if they have only 1 password.

3. Turn on two-factor authentication / 2FA

Turn on **two-factor authentication / 2FA** where you can for your online accounts.

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

This adds more security to your accounts.

4. Do regular checks of your accounts

Do regular checks of your other accounts for anything that looks strange.

It is a good idea to do this after an account has been breached.

This is just in case you have passwords that are:

- weak / easy to guess
- used for other accounts.

Examples of things that might be strange on your accounts might be:

- messages you did not send
- emails about trying to login.

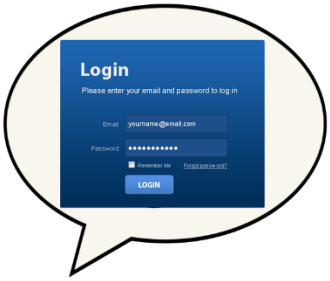
5. Watch out for phishing

Watch out for **phishing:**

- texts
- emails.

Phishing is when scammers send messages that look like they come from a real organisation.

Ways to tell a phishing message is fake include the email address not matching the organisation it came from.



Phishing messages:

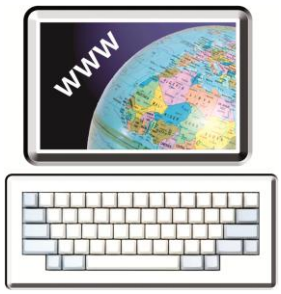
- ask for private information like login details
- give you a link to click.

A real organisation would not ask for that information.

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

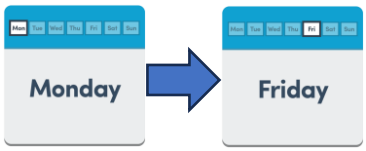
This website is **not** in Easy Read.

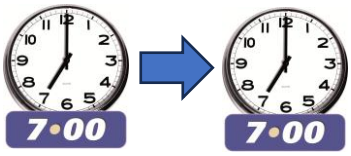
You can phone us if you need support making your report.

You can **phone** us on:

0800 114 115

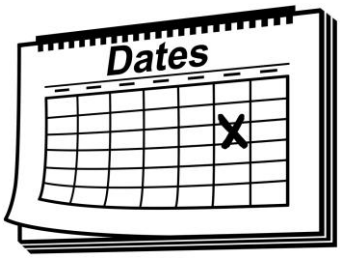
This number does not cost money to call.





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

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

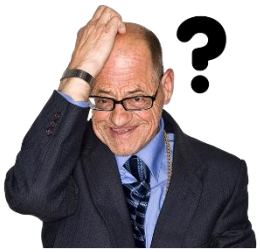
- Deaf / hard of hearing
- deafblind
- speech impaired / find it hard to talk.

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

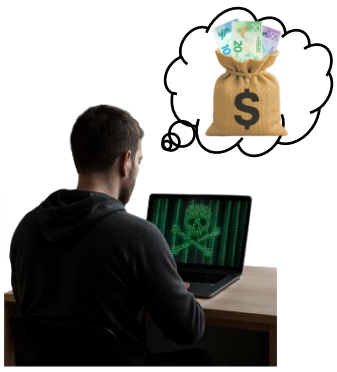
www.nzrelay.co.nz

Getting support after a data breach

Having your important information leaked might make you feel:

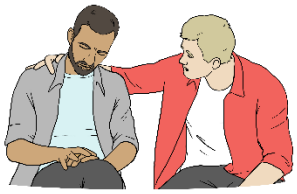


- embarrassed
- hurt
- confused.



Please remember attackers:

- make a living out of hacking data
- are very good at what they do.

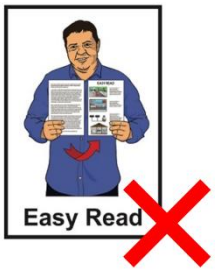


You are not alone.

There are support services you can use.

You can find more information about support services after a data breach at the IDCARE **website**:

www.idcare.org

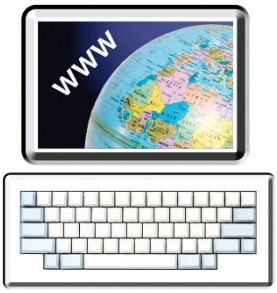


This website is **not** in Easy Read.

You can also **phone** IDCARE on:

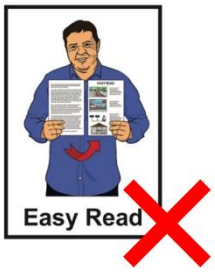
0800 121 068

This number does not cost money to call.



You can find more information about support services after a data breach at the Victim Support **website**:

www.victimsupport.org.nz



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

You can also **phone** Victim Support on:

0800 842 846

This number does not cost money to call.

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.