On this page:

The NDIA takes the protection of individuals' data and information security extremely seriously.

We have systems and processes in place to protect participants' and other stakeholders' information.

You can be a target of identity theft and fraud if your personal information is exposed in a data breach.

A data breach is when personal information is accessed, disclosed or used without authorisation.

Identity theft and fraud can have serious implications. This can include financial loss and emotional harm.

Previous large data breaches

For information on specific large data breaches, you can visit:

- HWL Ebsworth cyber incident
- Optus cyberattack
- Medlab cyberattack
- Medibank Private and AHM cyberattack
- Latitude cyberattack

How you can protect your personal information after a data breach

There are actions you can take to reduce the risk of harm if your personal information was accessed after a data breach.

1. Stay alert to increased scam activity, particularly email and SMS or telephone phishing scams. These scams look like they come from an organisation you know but are fake.
2. Do not click on any suspicious links or provide your passwords or any personal information. Always refuse any unprompted request from an individual to access your computer even if they

say they are from a credible organisation.
3. Change your online account passwords. Always use strong passwords. The Australian Cyber Security Centre has guides on good password practices.
4. Enable multi-factor authentication for your accounts where possible. This means using extra checks to prove your identity.
5. Install up-to-date anti-virus software on any devices you use to access your online accounts.
6. Monitor your bank account transactions and check your credit report to see if it has any unauthorised loans or applications.

For information on protecting your myGov, Centrelink, Medicare and Child Support accounts, visit the Services Australia website.

If you need more help

These organisations have useful information and support:

- Office of the Australian Information Commissioner for how to respond following a data breach.
- IDCARE is a national identity support service. Contact them for personalised support if you have concerns about your personal information.
- Scamwatch has information about all types of scams. You can report scams online.
- ReportCyber has information about online scams and how you can protect yourself online. If you believe your information has been misused because of a data breach, you can report this.

How the NDIA protects your personal information after a data breach

When a data breach happens, we take extra steps to protect your personal information and NDIS account.

These steps include:

- We will try to identify if you are affected by the data breach so that we can take appropriate actions.
- If you are affected, we may contact you with information about protecting yourself and supports available to you.
- We actively monitor your accounts for irregular activity.
- If we identify unauthorised activity on your account, we'll review it and take appropriate actions.
- We may take extra steps to verify your identity when you contact us. This is to make sure we are speaking with the right person.

You can find out more about how we handle your personal information in our Privacy Policy.

This page current as of
25 July 2023