24 April 2025

We are aware of a fraudulent email imitating an NDIS provider newsletter targeting NDIS participants.

Some participants may have received an email asking them to sign into the NDIS portal to update bank account details.

This email included a link which, if clicked, directs participants to a fake webpage where the user is asked to provide personal login details.

The NDIS will never ask you to click a link to update bank details through email, text message or direct message on social media.

What to do if you clicked the link in scam email

- Login to the NDIS participant portal via myGov or the myNDIS mobile app, and change your NDIS login details and myGov login details as soon as possible.
- Confirm that your bank details, phone number and email address are correct. If they are incorrect, contact us so we can help you update them.

Contact us

If you have been impacted by a scam and need support, please call the National Contact Centre on 1800 800 110.

How to know, spot and report scams

We want to help participants learn more about scams and fraud, especially how to know it, spot it and report it.

Understanding what scams are will support participants to protect their plans.

Be suspicious of unexpected contact or unsolicited requests for your NDIS details.

Please call the NDIS Fraud Reporting and Scams Helpline on 1800 650 717 to report a scam.

We are continuing to work with participants, their nominees and providers to make improvements to how we detect, prevent and respond to fraud in the NDIS.

Related articles

Scam alert – beware of malicious phishing email

Date
25 September 2020
Category

- News

Updating bank details

Date
6 July 2026
Category

- Fraud and compliance
- News

Phishing scams

Date
27 July 2026
Read more news