25 September 2020

Scammers are currently targeting providers with a malicious ‘phishing’ email.

Phishing scams are emails impersonating an organisation in order to trick the reader into providing confidential information.

Recent phishing emails falsely use the name of NDIA Chief Executive Officer, Martin Hoffman and request providers to update their details.

The email prompts you to open an attached PDF file that contains a link to a malicious website which then asks you to enter login usernames and passwords.

This website is fake, the emails are not from the NDIA and are not sent from a valid NDIS email address (@ndis.gov.au).

Agency advice to any provider that has provided information via this malicious email or website is to perform a password reset for all affected accounts. You should then review access logs to determine if your IT networks have been subject to unauthorised access or cyber intrusion.

Providers are strongly encouraged to consider advice from the Australian Cyber Security Centre to implement Multi-Factor Authentication which adds an extra layer of protection to personal and work IT accounts.

To report suspicious emails, or if you think you may have been scammed, you can call the NDIS fraud reporting and scams helpline on 1800 650 717 or email fraudreporting@ndis.gov.au

Visit our Scam awareness page to learn how to protect yourself from scammers.

Related articles

Category

- Fraud and compliance
- News

Phishing scams

Date
27 July 2026
Category

- News
- Notification

Scam alert – beware of emails asking you to update bank details

Date
24 April 2025

Scams Awareness Week starts on 17 August, 2020

Date
11 August 2020
Read more news