On this page:

A scam is an illegal trick. Scams usually try to get money illegally from people. A scam is a type of fraud.

Scams target people of all backgrounds, ages and income levels across Australia. All of us may be vulnerable to a scam at some time.

Scams succeed because they look like the real thing and catch you off guard when you're not expecting it. Scammers are getting smarter. They take advantage of new technology, new products or services and major events to create believable stories that will convince you to give them your money or personal information.

Our factsheet explains more about scams:

- What are scams? (PDF 162KB)
- Easy read - What are scams? (PDF 7.1MB)
- Easy read (text only) - What are scams? (DOCX 58KB)

We publish scams alerts if we become aware of scams targeting participants, nominees and providers.

We're introducing a new computer system and improving the way we work. As part of this, we will be sending SMS notifications to Agency-managed participants to confirm claims for services by providers who are not recorded in their plan. Find out about what we're doing next.

Transcript for 'Keeping your information safe'

Types of scams

Impersonation scam

Threat-based impersonation scams are common and can be traumatic for the victim. Typically, scammers pretend to be from a well-known trusted business, government department or organisation and they threaten you into handing over your money or personal details.

Participants have reported receiving calls from scammers pretending to be from the NDIA. The scammers will usually claim that there is a debt against your plan and that you will lose access to the NDIS if you don't provide them with personal information including bank details, addresses, and Medicare details. They may also ask participants to repay these 'debts'.

The call can sometimes appear to come from a legitimate provider. Scammers can sometimes 'spoof' a provider's phone number and it will show up on your phone. Sometimes these calls will come from a private number.

The NDIA will never call you and threaten to cancel your access to the NDIS because of a debt.

Invoicing scams

Scammers will sometimes send false invoices via email. These emails will often look like the real thing and will ask you to pay an invoice into an account that is different to the usual account you pay money into.

If you receive one of these emails, you should call your provider and ask them whether they sent this email. If they didn't, you should report it to us.

If you have accidentally paid the invoice, you should also:

- change your email account passwords
- contact your bank or financial institution and report the scam
- ask your bank whether they can reverse the payment, freeze the scam account and/or recover the funds
- check your NDIS records for any other unauthorised payments, withdrawals or updates.

Phishing scams

Phishing is a way that cybercriminals steal confidential information such as online banking logins, credit card details, business login credentials or passwords/passphrases.

They do this by sending fraudulent messages and emails (sometimes called 'lures').

Some phishing scams will claim to provide information on how to protect yourself against COVID-19, or how to claim a payment. If you click the link or open a document, a virus or malware will start to collect your personal information and data.

Phishing scams often impersonate government departments including the NDIA, Department of Health, Services Australia and the Australian Taxation Office.

Charity scams

Some scammers will contact you via phone, mail, email or face-to-face and pretend to be a charity. Often these messages will look like they real thing, but then they will ask you to click on a link, make a payment or provide personal information.

Before you donate to any charity you should always check if they are registered charity with the Australian Charities and Not-for-profit Commission Charity Register .

Unauthorised access

Scammers who have accessed your information illegally may use that information to make false claims against your plan.

Report a scam

The ACCC provides information to Australians about how to recognise, avoid and report scams.

To report a scam, visit Scamwatch .

If a scammer contacts you pretending to an employee of the NDIA or an NDIS provider, you should report it to us by:

- filling in our online tip-off form
  - this will assist the Agency in getting the important information we need to follow up properly and quickly
  - you will receive a reference ID once you have submitted the tip-off
- if you need help completing the online tip-off form you can call the NDIS Fraud Reporting and Scams Helpline on 1800 650 717.
- emailing fraudreporting@ndis.gov.au

Case study

Romance scam

Sandy had spent the past few months talking to a person named Bob through a popular dating app.

Sandy quickly starts developing romantic feelings for Bob and they arrange a time to meet for a date. A week before their scheduled date, Bob sends Sandy a message saying his car has broken

down and can’t afford to repair it. This means he will not be able to make their date.

Sandy tells Bob that she would be happy to pay for the repairs so he can still drive to their date and transfers a large amount of money to Bob. Within hours of this transaction, Sandy finds Bob’s online profile has been deleted and his mobile number disconnected.

Sandy realises she has been scammed and is distressed. She trusted Bob and shared personal information that she is now afraid will be misused. Sandy has concerns about her personal information being used to access her NDIS plan and calls the NDIS’ Fraud Reporting and Scams Helpline and tells the team what happened. The team reassures Sandy that she has done the right thing, and refers her to IDcare, who are able to provide her with professional counselling and assistance to help protect herself against identity theft.

After learning about Sandy’s situation, the NDIA’s team continue to monitor Sandy’s NDIS plan to check for any unauthorised activity or changes. This is to ensure the scammer has not accessed Sandy’s plan funds using her personal information.

Phishing

Maddie is the child representative for her son’s NDIS plan. Maddie receives a call from someone claiming to be from the NDIA. The caller asks Maddie to provide copies of her own personal identification documents. The person on the phone claims they lost her previous records and that they need new ones so Maddie’s son can continue having access to the NDIS. They state that if they do not get verified copies of the requested records, her son’s plan will be cancelled.

Maddie asks the person to ring back in half an hour. The caller demands Maddie send them the documentation immediately via an email address they provide. Becoming suspicious, Maddie ends the call.

Maddie calls the NDIA using the number provided on the website. The NDIA confirms that no one from the Agency has called and transfers Maddie directly to the NDIS Fraud Reporting and Scams Helpline (1800 650 717). The team instruct her to block the scammer’s number and advise her on what to do if she receives other suspicious calls in the future.

Maddie became suspicious of the caller when she felt pressured and threatened to do what they wanted. By using the NDIS website to find the official NDIS phone number, Maddie could be confident that she was talking to real Agency staff when she questioned the request. Even though Maddie didn’t give the scammer any personal information, the NDIA was still able to help by confirming the caller was a scammer and providing reassurance and advice. By following her instincts and taking action, Maddie was able protect her identity and her son’s plan.

Pretending to be the NDIA

John was sitting at home when his phone rang. He answered and was greeted by a man, claiming to be from the NDIA and wanting to talk about his plan.

John didn’t recall having spoken to the man previously, and didn’t think he was in need of a new plan.

As the conversation progressed, John became increasingly suspicious that the caller on the phone was not actually an NDIA staff member. As a result, he ended the call.

He then rang the NDIA to check if the call was legitimate. John was correct, there was no record of the NDIA calling John recently.

Upon receiving his call and being alerted to a potential scam, the NDIA increased security measures for John and his plan was monitored for any unusual or suspicious activity.

This page current as of
7 February 2024