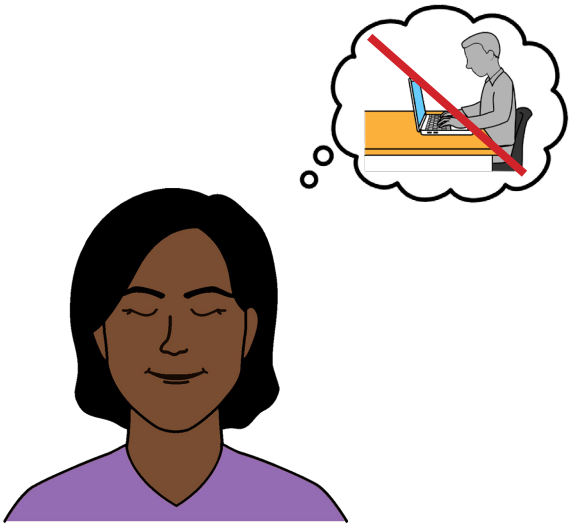


# How to stay safe from scams

Easy English

## Blue words

Some words in this book are **blue**.

We write what the blue words mean.

## Help with this book

You can get someone to help you

- understand this book

- find more information.

Contact information is at the end of this book.

# About this book

This book is about how to stay safe

from **scams**.


A scam is when someone tries to make you

- share your personal or account information
  - for example, your account password

or

- give away your money.

A person who does scams is called a **scammer**.

Scams can happen to anyone.

We want to help you stay safe from scams.

# What are types of scams?

## 1 Impersonation scams

An **impersonation scam** is when a scammer pretends to be from a real company.

For example, from

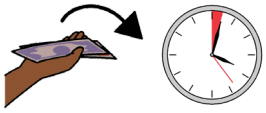
- your bank


- your internet provider

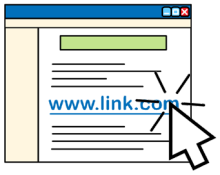
- the government.

The scammer might

- ask for personal information
  - for example, your date of birth



- tell you to send them money quickly




- tell you to click on a link


- send you a message on your phone asking for a passcode.

We will **never** ask you

- for your account information


- to log in to your account

- to give us a password or passcode.

## If you think someone is trying to do an impersonation scam


You can call the company to check if it was a real call or message.

For example, you can call us if the person said they were from Citi.

## Your one time PIN

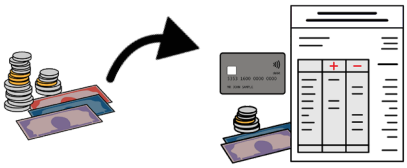
You might use a **one time PIN** when you sign in to your online account.


A one time PIN

- is numbers we send you in a text message

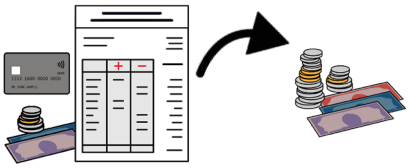
- helps to keep your account safe.

You might need a one time PIN or a password when you make some **transactions**.



Transactions are when

- money goes into your account



- money comes out of your account.

**Never** tell anyone your one time PIN or password.

We will **never** ask for your one time PIN or a password.

## 2 Goods not received scams

A **goods not received scam** is when a scammer tricks you to send them money.


The scammer might try to sell you a product or service that is **not** real.

The scammer might contact you through

- email or text message

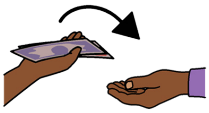
- social media.


The scammer might send you a link to a website.


The website might say you can buy something for a cheap price.

If you buy the product or service

- you will **not** get the product or service



- the scammer might take more money from you.

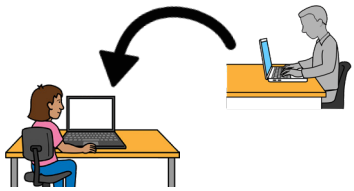
## 3 Remote access scam

A **remote access scam** is when a scammer tells you

- there is a problem with your computer or account

and

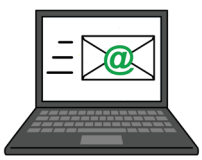
- they need **remote access** to your computer to fix the problem.



Remote access is when a person can control your computer with their own computer.

The scammer might contact you by

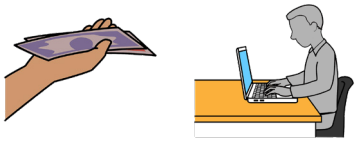
- text message



- email

- phone call.

## How do you know if you have been scammed?



You might have been scammed if you

- gave or sent money to someone you do **not** know

- gave your personal information to someone you do **not** know

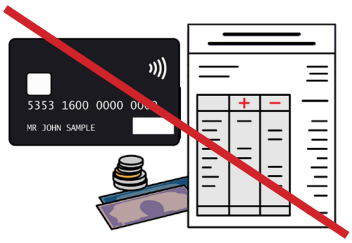
- see transactions from your account that you did **not** make.

You can call us to report anything you think might be a scam.

**Call**

1300 550 216

# What can you do if you have been scammed?




You can block your card so no one can use your account.


You can block your card

- online


- with our app on your mobile phone

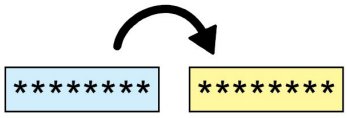
- by calling our Customer Service Centre.

If you are in Australia

Call 13 24 84

If you are in another country

Call +61 2 8225 0615




You should also change the password you use for your account online.

If you see transactions from your account that you do **not** think you made you can

- search the internet for the name of the company

or

- call our customer service centre.

Call 13 24 84

If you think you have been emailed by a scammer you can send it to us to investigate.

Email spoof@citicorp.com

# How to report or find out about scams

If a scam happens you can report it to the Scamwatch website.

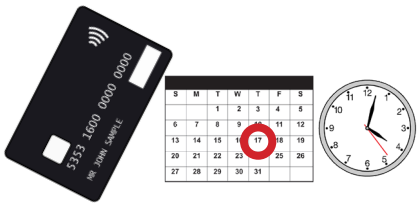
You can go to the Scamwatch website to read about scams that have been happening.

The Scamwatch website is run by the Australian government.

Website scamwatch.gov.au

# How we keep your account safe


We always check our website to see if there are ways we can make it more secure.




We show you what date and time you last used your account online.


You can check the date and time to make sure you were the last person to use your account.

## Two way alert service


If we think there is an unusual transaction from your account we can

- send you a text message

- call you

- send you an email.

You can reply to us and say if you made the transaction or not.

## More information

For more information contact us.

**Call** 13 24 84


**Website**

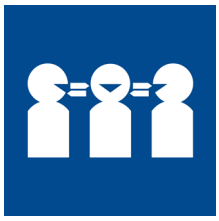
citibank.com.au

**You can read the full information on our website.**


**Website**

https://www1.citibank.com.au/help-and-support/scams

## If you need help with English



Our interpreters can help you with information on our products and services.

We understand that you might want to speak a language that is **not** English.

Our interpreters can speak many different languages.

You can call to get an interpreter to help you.

Call 13 24 84

**If you need help to speak or listen**

National Relay Service

Use the National Relay Service to make a phone call.

You must sign up to the service first.


Website accesshub.gov.au/nrs-helpdesk

Call 1800 555 660

This is a National Australia Bank Limited service, using certain trademarks temporarily under licence from Citigroup Inc. or as otherwise agreed by Citi and NAB.

National Australia Bank Limited (ABN 12 004 044 937, AFSL and Australian Credit Licence 230686) (“NAB”) is the credit provider and issuer of Citi branded credit products. NAB has acquired the business relating to these products from Citigroup Pty Limited (ABN 88 004 325 080, AFSL and Australian Credit Licence 238098) (“Citi”) and has appointed Citi to provide transitional services.

This Easy English document was created by Scope (Aust) Ltd. in June 2024 using Picture Communication Symbols (PCS).  For more information about the images, contact Scope on 1300 472 673 or visit scopeaust.org.au