

# ACT NOW, STAY SECURE

## QUICK REFERENCE GUIDE



### WHAT TO DO IF..

## YOU'VE BEEN SCAMMED

If in immediate danger call 000

Otherwise call:

AUSTRALIA IDENTITY THEFT HELPDESK

**1800 941 126**

or IDCARE:

**1800 595 160**



### 1. Act fast to stop any further losses

- Contact your bank or card provider immediately
- Change passwords on all devices and online accounts for banking, email, government and shopping

### 2. Get help to recover

IDCARE provide free help to make a plan to limit damage  
Call 1800 595 160

### 3. Warn others and report the scam to Scamwatch

### 4. Watch out for follow up scams

### 5. Install software updates regularly

### 5. Get support.

Visit: <https://www.scamwatch.gov.au/stop-check-protect/what-to-do-if-youve-been-scammed>

## GLOSSARY OF TERMS

### DATA BREACH

Any incident where unauthorised parties gain access to sensitive data

### ENCRYPTION

A method of scrambling information to make it inaccessible to unauthorized users

### IP ADDRESS

A number identifying any device connected to the internet

### AUTHENTICATION

The process of verifying a user's identity (sometimes in multiple ways) to avoid unauthorised access

# ACT NOW, STAY SECURE



## TIPS FOR STAYING SECURE

- ✓ **SETUP MULTIFACTOR AUTHENTICATION**
- ✓ **USE A PASSPHRASE (14+ CHARACTERS)**
- ✓ **HAVE MULTIPLE BACKUPS**
- ✓ **INSTALL UPDATES**
- ✓ **DEVALUE AND DELINK INFORMATION**
- ✓ **GET AN EMAIL FILTER**
- ✓ **PROTECT YOUR MOBILE DEVICE**

## PASSWORDS

### DOS

#### **CREATE STRONG AND UNIQUE PASSWORDS**

with over 14 characters and use 4 or more random words

#### **USE DIFFERENT PHRASES FOR EACH ACCOUNT**

#### **USE A PASSWORD MANAGER**

#### **USE MULTI-FACTOR AUTHENTICATION**

### DONTS

#### **SHARE PASSWORDS WITH OTHERS**

#### **WRITE YOUR PASSWORDS DOWN**

#### **CREATE LISTS OF PASSWORDS IN YOUR PHONE**

<https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases>

# ACT NOW, STAY SECURE



## TYPES OF SCAMS

- ✗ DATING AND ROMANCE SCAMS
- ✗ INVESTMENT SCAMS
- ✗ THREAT AND PENALTY SCAMS
- ✗ UNEXPECTED MONEY SCAMS
- ✗ BUSINESS SCAMS
- ✗ ONLINE SHOPPING CLASSIFIED AUCTION SCAMS
- ✗ CHARITY AND MEDICAL SCAMS
- ✗ PRIZE AND LOTTERY SCAMS

## WHAT ARE THEY AFTER?



### PERSONAL INFORMATION

Name, address, date of birth, demographic etc



### VOICE & FACIAL RECORDING

Your voice and face can be used in place of a password



### YOUR CREDIT INFORMATION

Bank, credit card, pension, superannuation or investment details



### YOUR IP ADDRESS

Your unique internet identifier

[www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information](http://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information)

## WAYS USED TO SCAM

**Remember – if something sounds too good to be true, it's probably a scam.**

- SMS / text message—Never click on links in text messages. Don't reply to messages from numbers you don't know. Call the organisation direct on a number you find.
- Phone—Let calls from unknown numbers go to voicemail. Hang up if you are not sure if the caller is who they say they are or if they threaten you. Call back on a number you find yourself.
- Computer—Don't give remote access of your computer to anyone.
- Email—Check if the email address is real. Contact the organisation directly from their website, not from a link.
- Website—Ask for a second opinion from advisor. Don't trust website reviews. Always do lots of research before giving any money away. Don't click on error message pop-ups. Use ABN lookup to check if stores are registered as a business. <https://abr.business.gov.au/>
- Social Media—always STOP, CHECK, ACT. Never send money or personal photos to a person you meet online. Research profiles and get a second opinion from someone you trust.

# ACT NOW, STAY SECURE



## QUICK LINKS TO GET HELP



### ACT NOW. STAY SECURE

<https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/act-now-stay-secure>

### OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

(Report a breach, make a complaint)  
<https://www.oaic.gov.au/>

### ACSC SMALL BUSINESS GUIDE

[https://www.cyber.gov.au/sites/default/files/2023-03/ACSC\\_Small\\_Business\\_Cyber\\_Security\\_Guide\\_V6.pdf](https://www.cyber.gov.au/sites/default/files/2023-03/ACSC_Small_Business_Cyber_Security_Guide_V6.pdf)

### MONEYSMART

<https://moneysmart.gov.au/#tools-and-resources>

### SCAMWATCH

[www.scamwatch.gov.au](http://www.scamwatch.gov.au)

### QUIZ – TEST YOUR SCAM SENSE

<https://www.scamwatch.gov.au/research-and-resources/quiz-test-your-scam-sense>

### IDCARE

<https://www.idcare.org/contact/get-help>

### SERVICES AUSTRALIA

Identity theft helpdesk 1800 941 126

### AUSTRALIAN CYBER SECURITY CENTRE – LATEST ALERTS AND ADVICE

<https://www.cyber.gov.au/>

### HOME AFFAIRS RANSOMWARE ACTION GUIDE

<https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf>

### THE LITTLE BOOK OF SCAMS

Available in audio book or can be downloaded  
<https://www.scamwatch.gov.au/research-and-resources/the-little-book-of-scams>

### LEARN THE BASICS

<https://www.cyber.gov.au/learn-basics>

### ABN LOOKUP

<https://abr.business.gov.au/> to check if business is registered

## STAY NOW ACT SECURE FACT SHEET



This project is supported with funding from the Australian Government's Department of Home Affairs