IDcare

Safety takeaways

Help protect yourself from cyber criminals.

By taking a few simple steps, you can significantly reduce your risk and help keep your identity and money safe.

Sponsored by:

Westpac ANZ

"Our mission is simple: to give people back a sense of control, dignity, and justice in the face of cybercrime and scams."

— Dr. David Lacey, Founder & Group CEO, IDCARE

Protect Your Identity

It's Worth More Than You Think!

Your identity is valuable. If a scammer gets hold of it, they can use it to steal your money, open accounts in your name, and cause serious harm to your life.

Many people don't realise how easy it is for this to happen, or how hard it can be to fix. This guide shares simple, practical steps to help you protect your personal information and stay safe from scams and identity theft.

Contents

So you've been scammed

The Three-Step Response

Step 1

Contact your bank or financial institution

Step 2

Contact IDCARE, our service is free and confidential

Step 3

Talk to someone - scams thrive in silence

Stop. Check. Protect.

"I can't believe what I did... within minutes, I'd done what they asked, and about an hour later I thought, 'What on earth did I do that for?'"

Your best defence against scams is to slow down.

Scammers rely on catching you when you're:

- Busy
- Stressed
- Distracted

That's when you're less likely to think clearly. They use pressure, fear, and urgency to push you into quick, risky decisions.

Stop. Check. Protect.

Take a moment.

Ask yourself — does this feel right?

Get advice.

Double-check the details.

Slowing down is one of the simplest and strongest ways to stay safe.

Remote Access

These scams aim to take control of your device and access your private information.

They often start by grabbing your attention:
– A pop-up warning about viruses or hackers
– Red flashing messages, sometimes with a loud alert
– A phone call pretending to be from your “bank”, phone company or internet provider saying there is something wrong on your account.

From there, you may be directed to a **fake ‘helpline’.**
The person on the line may sound helpful, but their goal is to get you to download software — giving them remote access to your device.

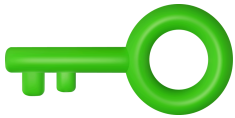
Once they’re in, they can:
– Steal your passwords
– Access your bank accounts
– Lock you out of your own files

Never allow remote access unless you’ve contacted a trusted provider yourself.

Think you’ve allowed remote access?

Act fast:
– Disconnect from Wi-Fi immediately
– Contact your financial institution right away
– Seek trusted technical support

Passwords



Passwords are your first layer of protection online.

Using the same one for every account might be easy — but it's risky.
If one is hacked, scammers can get into everything.

We now manage around **100 passwords each** — it's impossible to remember them all.

What makes a good password?
– **Long** (12+ characters)
– **Complex** (letters, numbers & symbols)
– **Unique** (different for every account)

Avoid simple tweaks of the same password — scammers spot patterns quickly.

How do you keep track?
Use a **password manager.**
It stores your passwords securely, fills them in when needed, and creates strong new ones.

- Apple: iPhones and iPads come with a built-in **Passwords app.**
- Android: Most Android phones have **Google Password Manager.**

There are also free and paid apps - just do your research.

Quick tip:
When your browser asks to "save password," it's safer to say no. Use a password manager instead — it's much more secure.

Multi-Factor Authentication

While many banks automatically set up multi-factor authentication (MFA) to protect your financial accounts, it's important to enable MFA on your other accounts, like social media and email, to protect all your personal information.

How MFA works:

- First, you log in with your username and password.
- Then, MFA asks you to verify your identity with something extra, such as a code sent to your phone or an authentication app.

Why MFA is crucial:

- Even if someone gets hold of your password, they won't be able to access your account without the second factor.
- It adds an extra layer of protection against phishing, hacking, and scams.

Where to enable MFA:

- **Social Media:** Go to your account settings (usually under "Security" or "Privacy") and look for the option to enable two-factor authentication (2FA). Popular platforms like Facebook, Instagram, and Twitter offer this feature.
- **Email:** Most email providers, like Gmail or Outlook, allow you to set up MFA in your account security settings.

Credit Reports

What is a Credit Report?

Your credit report is a summary of your credit history. It shows:

- What credit you've applied for
- What credit you've been given
- Your repayment history (including missed or late payments)
- Defaults or serious credit infringements
- Bankruptcies or court judgements (if any)

It's used by banks, telcos, and lenders to decide whether to lend you money or offer services like a phone plan.

Why should I check my Credit Report?

Checking your credit report every 6-12 months can help you:

- **Spot fraud or scams** (i.e. loans taken out in your name)
- Fix errors (wrong info can lower your credit score)
- Track your financial health (see how lenders view you)

Checking your own report does NOT affect your credit score.

Credit Reports
continued

How to check your credit report for free:

There are **three credit reporting agencies**. You can request a **free copy every 3 months.** You need to get a report from **each** agency to get a complete picture of your credit history.

1) **Equifax** www.equifax.com.au
- What you'll need: ID (like driver licence, Medicare Card, passport.
- Usually delivered within 10 days.

2) **Experian** www.experian.com.au
- What you'll need: same ID requirements
- Online request or download form

3) **Illion** www.illion.com.au
- Same process - easy online form
- Can send by email or post

What if something is wrong?
If you see:
- Credit you didn't apply for
- Loans you didn't take out
- Payments marked late when you paid them on time

Contact the credit agency AND provider (like the bank or telco)

IDCARE

Concerned about identity theft, scams and cybercrime?

Regain Control with IDCARE

Every year, over **1 million Australians** are impacted by scams, cybercrime, and identity theft.

If you're affected, **don't feel embarrassed** - you're not alone.

IDCARE is a **free national identity and cyber support service.**

Our **expert Identity and Cyber Security Case Managers** offer **personalised, free support** to help you regain control and recover.

Contact Us

1800 595 160

www.idcare.org

IDCARE can help if you:

- ✓ Discover someone is using your identity
- ✓ Click on the wrong link
- ✓ Visit a fake website
- ✓ Answer the wrong call
- ✓ Provide personal information to a criminal
- ✓ Lose your wallet
- ✓ Have your house broken into
- ✓ Discover your mail has been stolen
- ✓ Become involved in a relationship or investment scam