Scams and cyber risks

What to look out for and where to seek help if something doesn't feel right

A note before you read on

We've put this guide together because financial harm can happen to anyone, including people who are careful, experienced, and well-informed. It's not a reflection of you or your judgment. It's a reflection of how sophisticated these schemes have become. Sometimes the people who cause financial harm are very convincing. They can present themselves as trusted advisors, use professional-sounding language and offer arrangements that seem legitimate at first.

If anything in this guide resonates with your situation, even in a small way, please know that help is available and reaching out generally costs nothing.

What financial harm can look like

Financial scams and fraud are increasingly common in Australia. They are often designed specifically to look trustworthy. Below are some patterns that have affected many Australians in recent years.

Unofficial or unregistered investment schemes

These may be described as superannuation opportunities, managed funds, property investments or exclusive investment programs. They often:

- Are introduced through a trusted connection, an online acquaintance, or someone presenting as a financial advisor
- Offer strong or guaranteed returns
- Ask you to transfer money directly to a private account rather than a regulated financial institution
- Have no formal portal, statement, or regulated account where you can independently verify your balance
- Become harder to contact over time, or make it difficult to withdraw your money.

Advisors and contacts who are not who they seem

Legitimate financial advisors in Australia must be registered with ASIC and hold an Australian Financial Services Licence (AFSL). If someone is giving you financial advice but cannot provide these credentials, or discourages you from checking, that is a significant warning sign.

Scammers may also impersonate real companies, advisors, or even government agencies, using similar names, logos, or websites to appear credible. Contact that begins unexpectedly, whether by phone, email, or online, deserves extra caution.

Impersonation scams

Scammers sometimes pretend to be legitimate organisations, including banks, lenders, government agencies or other trusted service providers. They may use official-looking logos, email addresses, websites or phone calls that appear genuine. They might ask you to click on a link, log into an account, update personal information or transfer money urgently. If you receive an unexpected request, particularly one that creates a sense of urgency, it is safest to stop and independently verify it using contact details you already know to be genuine.

Requests to move or transfer money

This can include sending money overseas, purchasing gift cards or cryptocurrency on someone's instruction, or transferring funds to an unfamiliar account. Once money leaves your account, particularly internationally, it can be very difficult to recover. Legitimate institutions should not pressure you to transfer money immediately without giving you an opportunity to independently verify the request.

Pressure, urgency, or secrecy

Scammers often create a sense of urgency or ask you to keep an arrangement private. Being discouraged from seeking a second opinion, speaking to family, or taking time to think is a warning sign in itself.

> ***"I didn't think it was a scam — it seemed so real."***
>
> This is one of the most common things people say after experiencing financial fraud. Scams succeed because they are designed to. The people behind them are sophisticated, patient and convincing. Australians lose billions of dollars to them every year, across every background and age group. There is no typical profile of someone this can happen to.

If something doesn't feel right — what to do

If something doesn't feel right, trust your instincts and seek advice promptly. The organisations below offer free, confidential support and may be able to help you protect your identity, stop further losses, and assist with recovery. You do not need to be certain something is wrong to seek support, and making contact does not commit you to any course of action.

1

Get expert identity & scam support (Free)

IDCARE — National identity and cyber support

Website: https://www.idcare.org

Phone: 1800 595 160

IDCARE provides free, confidential support for people affected by scams, identity theft or cyber incidents. They can help you understand what has happened, create a personalised recovery plan, and reduce further risk, without any pressure or judgment.

2

Report the scam

ScamWatch (National Anti-Scam Centre)

Website: https://www.scamwatch.gov.au

Advice on how to protect yourself from scams and what to do if you've been scammed. Reporting what happened helps protect other Australians. ScamWatch also provides current alerts and advice on scam types.

3

Report cybercrime or online fraud

Australian Cyber Security Centre (ACSC) – ReportCyber

Website: https://www.cyber.gov.au

Phone: 1300 292 371

Report hacking, identity theft or online fraud. You'll receive guidance on what to do next and your report may assist law enforcement.

4 Contact your bank(s) or lender(s) immediately

If you think your accounts or personal information may have been compromised, contact us or your bank or other financial institution as soon as possible. They can help:

- Secure your accounts
- Investigate unusual transactions
- Put additional protections in place

Acting quickly can significantly improve the chances of stopping or reversing losses.

5 Government support if your identity documents are affected

Services Australia (myGov, Medicare, Centrelink)

Phone: 13 24 68

Can help secure your government accounts and fix records if your details have been misused.

ID Support NSW (if you live in NSW)

Website: https://www.nsw.gov.au/id-support-nsw

Phone: 1800 001 040

Provides help replacing identity documents and recovering from identity theft.

6 If you need to make a complaint about a financial service

Australian Financial Complaints Authority (AFCA)

Website: https://www.afca.org.au

Phone: 1800 931 678

If you are not satisfied with how a financial institution has handled your situation, AFCA provides a free, independent complaints service.

7 Look after your wellbeing

Concerns about money — whether or not anything has gone wrong — can be stressful and unsettling. If you're finding it difficult, support is available:

Lifeline: 13 11 14 (24/7)

Beyond Blue: 1300 22 4636

How Inviva will communicate with you

To help keep you safe, it's important to know what you can expect from us.

- We will never ask you to tell us your password by email, text message or phone.
- If someone contacts you claiming to be from Inviva and asks for your password, do not proceed and contact us using the details on our website or your statements.
- If we ask you to complete an action online, we will direct you to our secure customer portal or ask you to contact us using the details published on our website.
- If you receive a message claiming to be from Inviva that seems unusual, unexpected or urgent, please contact us directly using our phone number 1300 222 223. You can independently confirm this phone number on your statements or on our website before taking any action.

Quick checklist

- Contact your bank or lender immediately if you are concerned about transactions or identity theft
- If you think your accounts may have been compromised, change your passwords and enable additional sign-in security, such as one-time verification codes, where available
- Use a different password for each of your important online accounts
- If you think you've been compromised, contact IDCARE for free, confidential and tailored support
- Report actual or likely scams to Scamwatch
- Report any actual or suspected cybercrime to ReportCyber
- Monitor your accounts and credit file.

You're not alone — and you don't have to figure this out by yourself.
Support is available at every stage, and acting quickly can make a real difference.

inviva