

Legal Yarns

Identity Theft & Scams





Protecting our mob from identity theft and scams

What is identity theft?

Identity theft is when someone steals your personal information (online or physical) without your consent and uses it to steal money, commit fraud, or other crimes for their benefit. Often it is a time pressured situation where scammers will make you feel like you have to act urgently. This can happen to anyone - one in four Australians have had their identity stolen sometime in their life. This legal yarn provides some guidance as to what to do if this happens to you, and how you can try and protect yourself against it.

What happens when my identity is stolen?

The impact of having your identity stolen can be devastating and take time to fix. It can be difficult to prove who you are and impact your ability to get your identity documents replaced or renewed. It may affect your ability to apply for a loan because your credit rating has been impacted and impact your overall financial stability. This is why it is really important to **act quickly** as soon as you think you may have had personal information stolen either online or physically.

What is covered in this Legal Yarn?

We take you through the following issues so you know what to look out for, and how to protect yourself against identity theft.

1. What is identity theft? (see page 2)
2. What happens when my identity is stolen? (see page 2)
3. What does identity theft and scams look like? (see page 2)
4. How do I protect myself from getting scammed? (see page 3)
5. What do I do if my identity is stolen? (see page 3)
6. Resources and Support (see page 3)

What does identity theft and scams look like?

It is important to know common ways in which you can be scammed and your identity stolen. You can also check out our Legal Yarn on Online Safety tool. Your personal information can be stolen from you in various ways. This can include:

- Financial information such as bank account details and tax file number. This may result in your bank card being used for purchases you have not authorised.



Identity Theft & Scams



- Personal information such as date of birth and contact details. This may result in you receiving text messages, phone calls or messages on social media asking you to transfer money, confirm your identity or change your password.
- Identity documents such as drivers licence and passport. This may be used in combination with the above to use obtain a financial advantage.

These days, it is common for scammers to call you and try to trick you into handing over your personal and financial information over the phone. They often use sophisticated methods to achieve this and it can be difficult to know when this is happening. It is important to remain aware of this possibility when accepting phone calls from numbers you do not recognise.

It is also common for identity theft or scams to take place when there has been a data breach. Data breach is when sensitive or personal information that is held by an organisation or company is accessed, disclosed or exposed to unauthorised people either accidentally or through a data breach. In instances where this has occurred, the organisation will immediately inform you and also provide recommendations for how to protect yourself.

How can I protect myself from getting scammed?

There are ways that you can try and protect yourself from having your identity stolen. You can:

- Have a strong password that you change regularly
- Set up two factor authentication
- Do not share your personal information over the phone or online if you are feeling pressured or harassed by someone.
- If you are sure you can always call the organisation back on their publicly available contact number and double check, or you can ask them to send an email, that way you can verify the request.

As an example, if someone says that work for the ATO Centrelink or another organisation and are pressuring you to make a payment do not make the payment. Call the ATO on their publicly listed number and check the call is legit.

If you're unsure what two factor authentication (2FA) is, it is an extra step to help keep your account safe. When you log in, you need to prove it's really you in two ways. For example, you might get a code by text message, or use an app like Google Authenticator or Microsoft Authenticator to get a code.

What do I do if my identity has been stolen?

As soon as you suspect that your identity may have been stolen you should act immediately.

If you notice unusual activity on your bank transactions that you don't recognise you should:



Identity Theft & Scams



1. Call your bank immediately and ask to put a block on your accounts. You should make a police report (if your physical card has been stolen) as well as making a report with ASIC.
2. Change your passwords and pins immediately and ensure you have multi-factor authorisation to secure your accounts.
3. Visit the Australian Cyber Security Centre's dedicated webpage and resources on identity theft
4. Contact IDCARE who provide National Identity and Cyber Support to individuals, businesses and organisations who have had their security compromised.

Where can I get help?

Call us at VALS on 1800 064 865 or check out [our website](#) for more information or legal support.

- The [Australian Cyber Security website](#) has resources and support regarding identity theft: <https://www.cyber.gov.au/threats/types-threats/identity-theft>.
- IDCARE provides provide National Identity and Cyber Support to individuals, businesses and organisations who have had their security compromised: <https://www.idcare.org/>.
- The Little Book of Scams for First Nations peoples has been developed by Scamwatch and provides resources and information: <https://www.scamwatch.gov.au/research-and-resources/resources/resources-for-first-nations-peoples#toc-the-little-book-of-scams>

Disclaimer

This document contains general information only and does not constitute legal advice or services.

This fact sheet was published in September 2026. All information is accurate as of date of publication. For further information please head to VALS website.

