

We can **help**
if your identity
is stolen



Each year more than 150,000 Australians are victims of identity crime. If your NSW Government proof of identity documents or credentials are stolen or fraudulently accessed, it can be hard to know where to start. That's why ID Support NSW is here to help.



What is identity crime?

Identity crime happens when a scammer gains access to your personal information without your consent. It can happen online, offline, or a combination of both. In most cases, identity crimes involve scammers stealing money by pretending to be someone else, like you.

Identity crime can impact your personal finances. Until the issue is resolved, this could make it difficult for you to get phone contracts, credit cards or a mortgage.

Around 1 in 4 Australians have been a victim of identity crime at some point in their lives.

How identity crime can happen

There are many ways for your identity to be compromised, including:

- phone calls
- text messages
- emails
- fake profiles
- and other communications.

Scammers often pretend to be from a charity, a bank, a service provider or even the government.

Once they have your personal information, they can then fraudulently apply for credit cards or loans in your name, make illegal purchases, gain access to your bank or email accounts, tax file number or superannuation, change your mailing address and more.

If you get a call or message claiming to be from a business or organisation and something doesn't feel right, contact them separately, using the details on their official website. You can ask them to confirm if the contact is legitimate.

Introducing ID Support NSW

The NSW Government established ID Support to help people learn more about and prevent identity crime. We can help you improve the security and safety of your personal information, and support you if any of your NSW Government proof of identity credentials have been compromised. These include:

- Driver licence
- Birth certificate
- MyServiceNSW Account
- Security licence
- Firearms licence
- Working with Children Check
- Seniors Card.

We will continue to expand our services to help with other types of compromised documents.

What we do

If your identity falls into the wrong hands, ID Support can provide advice on how to:

- recover the security of your identity
- protect your identity in the future
- find support, including counselling services.



Common scams

Scams are always evolving and becoming more sophisticated and convincing.

Scams are often delivered by:

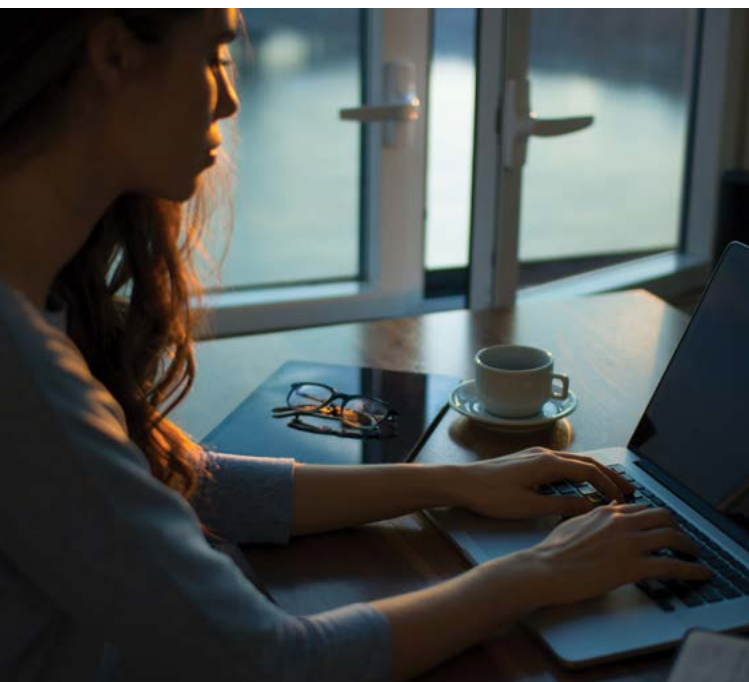
- email – often asking you to click a link which will compromise your device. Be wary if it's an organisation you don't do business with. Check for poor spelling and grammar, strange or blurred logos, poor formatting.
- text messages – will often have a link which will access your device and your contacts. Many suggest urgency, or a common situation such as a parcel delivery (asking you to pay the delivery fee).
- phone calls – situations are often unrealistic, and may come from robots/auto-diallers. A common scam is that your credit card is about to be charged and you're being given a chance to opt out, then asking you to provide your card details.

Warning signs

- You stop receiving mail at your address, especially bills and statements.
- You can't log in to your online accounts.
- You receive bills, invoices, or receipts for goods or services you didn't request.
- Your passwords appear to change without your permission.
- Bank or credit card statements include items you don't recognise.
- Devices or online accounts are accessed by third parties.
- Accounts show overseas transactions that you didn't make.
- Your superannuation balance is much lower than expected.

How to protect your identity online:

- Don't open unusual or unexpected texts or emails.
- Hover over links and if you don't recognise it, or if it looks suspicious – don't click on it.
- Don't give your details to unknown websites or websites you don't trust.
- If you're asked to provide your credentials, take action through the official website and not through unknown links.
- Choose strong unique passwords for all your accounts and change them regularly.
- Use complex passphrases that are easy to remember but also contain upper and lowercase letters, numbers and symbols so they're hard to crack.
- Add multi-factor authentication on accounts.
- Be curious about your information being collected by organisations.
- Remember that you have a right to know and ask how your information is used.



How to protect your identity offline:

- Secure your personal credentials at home and when travelling, don't write any credentials down on paper.
- Put a lock on your mailbox and securely destroy any documents you don't need if they have personal information.
- Be cautious about requests for your personal information over the phone and in person.
- Never give out personal information over the phone, especially if the caller is unknown or asking for payment.
- Order a free annual copy of your credit report from a credit reporting agency.
- Regularly check your bank and superannuation statements.
- Be curious about your information being collected by organisations.
- Remember that you have a right to know and ask how your information is used.
- If you receive a call requesting information or credentials, finish the call and call the service back using their official and publicly listed phone number.

Be cautious about requests for your personal information over the phone and in person.

Get in touch

We have a dedicated support team who provide advice and solutions for your compromised NSW Government identity credentials.

Call us on **1800 001 040**
Monday to Friday, 9am to 5pm

To find out more visit **nsw.gov.au**



**Your identity is important.
Let's protect it.**