



# How to protect your identity

**Identity theft can be stressful, costly and take time to resolve.**

**As more services move to digital spaces, it's important that you feel confident that your identity is protected – and that you understand how to keep yourself safe online.**

## About identity theft

Identity theft is when a criminal gains access to your personal information without your consent.

They can then run up debts in your name by fraudulently applying for phone contracts, credit cards or loans. Scammers can also make illegal purchases, gain access to your bank or email accounts, change your mailing address and more.

Whether it happens online, offline, or both, the damage can be serious. Identity theft can impact your personal finances. Until it's resolved, this can make it difficult for you to get loans, credit cards or a mortgage.

Around 1 in 4 Australians have been a victim of identity theft at some point in their lives. On average, they lose more than \$4000.

## How to prevent identity theft

Here are some simple steps you can take:

- Only take the ID you need when you go out and keep it in a secure place.
- Use a digital wallet for your payments and ID cards where possible.

- Lock your devices with a passcode, passphrase and/or biometric (such as fingerprint or facial recognition).
- Use long, complex passphrases by combining multiple words into a string that's easy for you to remember. It should contain a good mix of upper and lowercase letters, numbers and symbols, to make it harder to crack.
- Avoid using public Wi-Fi where possible and when needed use a Virtual Private Network (VPN).
- Secure your browser – visit [cyber.gov.au](https://cyber.gov.au) for more information.
- Don't provide personal or financial information via social media, text or email.
- Set your social media profiles to private and limit the amount of information you share on them.
- Review the privacy policies of companies to understand how your data will be used, stored and protected, and ask what they do and don't need to keep.
- Use multi-factor authentication on digital services where it's available, such as getting a code sent to your phone by SMS before you can log in to your account.
- Don't click links or popups you didn't request or weren't expecting.
- Regularly review your bank statements and credit reports, and sign up for alerts with your banks and creditors to ensure early detection of any identity theft.
- Use a cross-cut shredder when destroying any documents with your personal info.

If your identity documents have been stolen or compromised, please contact ID Support NSW. You can call **1800 001 040**, or use our online form at [nsw.gov.au](https://nsw.gov.au)



## How to recover your identity

If you're a victim of identity theft, it can be hard to know where to start. But it's important to act quickly.

Follow these steps:

### Notify your financial institutions

Report the breach as soon as possible. Request extra security measures for your accounts such as placing a block on your account, closing it or adding passwords and PINs.

You can also tell other money transferring institutions such as PayPal, Western Union and Gumtree about what happened.

### Check your credit reports

Visit [moneysmart.gov.au](https://moneysmart.gov.au) to check your free credit score and credit report.

This means you can see if there has been any unfamiliar activity in your name, including:

- credit applications you never made
- accounts you never opened
- enquiries you never made
- personal information you never provided.

The website also provides the contact details for the three main credit reporting agencies. You can contact them if you want to know more about your credit report or how to place a block on credit applications in your name.

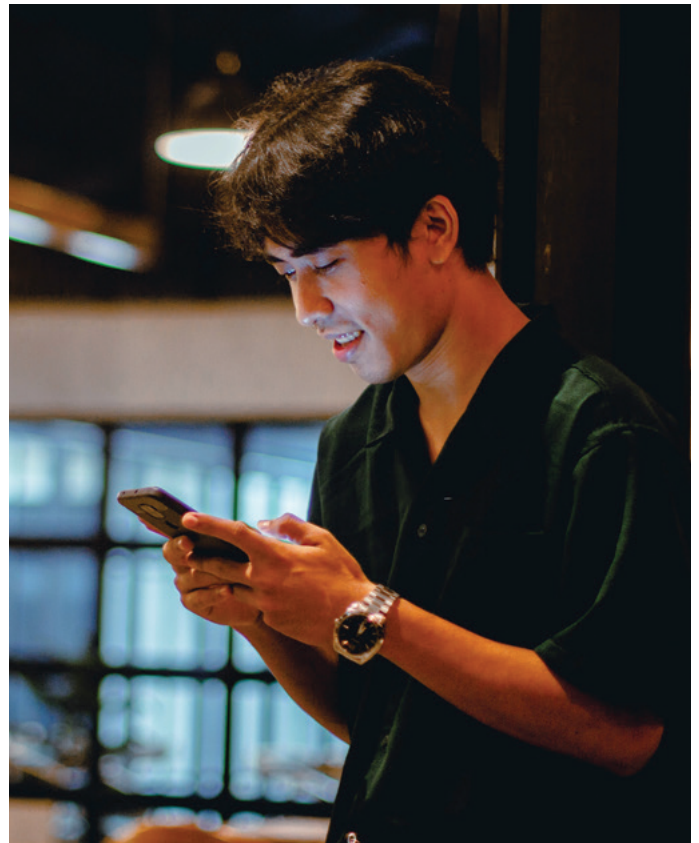
### Freeze your credit

Freezing your credit means that credit reporting agencies can't disclose your personal information to credit providers unless you give them your written consent, or they're required by law to do so. A ban also prevents accounts being opened in your name.

### Submit a police report

Visit [cyber.gov.au](https://cyber.gov.au) and submit a report. This will be assessed by the appropriate police jurisdiction. You'll need to provide personal information and details of what happened, including dates and relevant financial transactions.

After you submit your report, you'll receive a receipt with a unique Report Reference Number. You can provide this number to financial institutions or other organisations as proof that the breach has been reported to police. You may be contacted by police for more information.



### Change and strengthen passwords

Change all your important passwords. Don't use obvious or identifying information like your date of birth. Use complex passphrases that are easy for you to remember but hard for hackers to crack. Make sure you include upper and lowercase letters, numbers and symbols. It's also important to use different passphrases for different accounts (email, banking, social media etc).

### Establish multi-factor authentication

Multi-factor authentication (MFA) is a security measure that requires 2 or more security steps. MFA typically requires a combination of something you know (such as a password, PIN, or secret question) and something you possess (such as an access code generated by an authenticator app, or a verification text or email). This reduces the risk of others accessing your account.

### Replace your identity documents

If your NSW Government proof of identity documents or credentials are stolen or compromised, you may need to cancel and replace them. This can prevent your ID being fraudulently used.

If your identity documents have been stolen or compromised, please contact ID Support NSW. You can call **1800 001 040**, or use our online form at [nsw.gov.au](https://nsw.gov.au)



ID Support NSW