

Introduction

What is identity theft?

Identity theft is a type of fraud that involves the use of someone's personal information. Identity theft can occur online or offline, or a combination of both. Common credentials targeted include driver licences, passports, Medicare cards and bank account details.

Common signs of identity compromise and misuse include:

- Lost or stolen identity credentials (e.g. passport, driver licence).
- Mail stops arriving at your address.
- Bills, invoices or receipts are addressed to you for goods or services you haven't asked for.
- Legitimate applications for credit are unexpectedly declined
- Debt collectors contact you regarding purchases or loans that you did not make.

Responding to identity theft

Every case is different, but here are some general tips on how you can respond:

- ☐ Update and run anti-virus software on all internet-enabled devices.
- ☐ Reset all passwords and PINs.
- ☐ Review where you keep your personal information or images of identity documents on your devices, such as within your emails or stored on your hard drive and remove unnecessary items.
- ☐ Review your existing accounts. Look for unauthorised transactions, changes to settings (for example email forwarding rules), and, if possible, the times and locations your account has been accessed.
- ☐ Check your [credit report](#) to see if someone is accessing credit in your name.
- ☐ Contact your financial institution and let them know what has happened and ask how they can assist.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Mitigating the risk of identity theft online

- ☐ DO NOT respond to suspicious texts or emails, or click on any links within the message.
- ☐ Never send money, credit card details, online account details, or copies of personal
- ☐ Choose passwords that would be difficult for others to guess and update them regularly. Consider using a password manager.
- ☐ Secure your networks and devices with antivirus software, ensure your device firewall is enabled.
- ☐ Be cautious when using social media and limit the amount of personal information you publish online.
- ☐ Be cautious about requests for your personal information over the internet.

Mitigating the risk of identity theft offline

- ☐ Secure your personal documents at home and when travelling.
- ☐ Put a lock on your mailbox and destroy any documents containing personal information not required.
- ☐ Be cautious about requests for your personal information over the phone and in person.
- ☐ Order a free copy of your credit report from each [credit reporting agency](#), available every three months.
- ☐ Regularly check your bank and superannuation statements.
- ☐ Be curious about where your information goes that is collected by organisations – you have a right to know why they are collecting it, how they will secure it, for how long they will keep it, and whether they will share it.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.