





Understanding Identity Theft

Understanding identity theft




Identity theft is a type of fraud that involves the compromise of identifying information that may or may not result in the misuse of such information by another person without authorisation. The theft of identifying information is also referred to as an “identity compromise”. The further usage of compromised information is also referred to as “identity misuse”. Identity theft can occur online or offline or a combination of both. Common information targeted includes driver licences, passports, and account details.

Common signs of identity compromise and misuse





-  Lost or stolen identity credentials (e.g. passport, driving licence).
-  Mail stops arriving at your address.
-  Items appear on bank/credit card statements you don't recognise.
-  Bills, invoices or receipts addressed to you for goods/services you haven't asked for.

Responding to identity theft:

Every case is different, but here's some general tips on what to do:







-  Contact IDCARE to assess your risks and build a tailored response plan.
-  Update and run anti-virus software on all Internet-enabled devices.
-  Reset all passwords and PINs.








-  Review where you keep your personal information on your devices, such as emails and hard drive and remove unnecessary items.
-  Review your existing accounts. Look for unauthorised transactions, changes to settings (for example email particulars), 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's happened and ask how they can assist.

Understanding Identity Theft

Mitigating the risk of identity theft online

-  DO NOT open suspicious texts or emails – delete them.
-  Never send money or give credit card, online account details or copies of personal documents to anyone you don't know or trust - and never by email.
-  Choose passwords that would be difficult for others to guess, and update them regularly.
-  Secure your networks and devices with antivirus software and a good firewall.
-  Be cautious about 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 a credit reporting agency annually.
-  Regularly check your bank & 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, whether they will share it.

Other fact sheets

- | | | |
|---|--|--|
|  Credit Reporting Agencies |  Engaging Organisations |  Devices and Technology |
|  Scam Prevention and Education |  Social Media |  Your Rights |

Disclaimer © 2018 Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this FACT SHEET, IDCARE disclaims any liability to any person in respect to any actions performed or not performed as a result of the contents of the alert or any accompanying data provided. Note our service is free to the community and our Counsellors will never ask you to provide your personal information and credentials if we make contact with you.

