Business Local

A Small Business Development Corporation service funded by the Government of Western Australia

Identity theft

Identity theft occurs when a criminal gains access to your personal information (such as your name, address, date of birth or bank account details) to steal money or gain other benefits. Even if you think thieves only have a small amount of information about you, they can use it to find more information about you, including photographs, your date and place of birth and even information about your family. This can be enough to apply for services, such as a new bank account. They can also use your personal information to create fake identity documents in your name or even apply for real identity documents in your name, but with another person's photograph.

How does identity theft occur?

Criminals may attempt to gain your personal information using a number of different techniques, including:

- 'phishing' - you may provide personal information over the phone or internet to what appears to be a legitimate business, but is actually a scam,
- hacking into your online accounts,
- retrieving your personal information from social media, and
- illegally accessing information about you which is stored on a business database.

What can happen as a result of identity theft?

If a criminal steals your identity, they may use it to:

- trick your bank or financial institution into giving them access to your money and other accounts,
- open new accounts and build up debts in your name which can ruin your credit rating,

P 08 9071 5142 | F 08 9072 1693 | W esperancecci.com.au
A 26B, 91 Dempster St Dutton Arcade | PO BOx 817 Esperance WA 6450

- take control of your accounts, including by changing the address on your credit card or other accounts so you don't receive statements and don't realise there is a problem,
- open a phone, internet or other service account in your name,
- claim government benefits in your name,
- lodge fraudulent claims for tax refunds in your name and preventing you from being able to lodge your legitimate return,
- use your name to plan or commit criminal activity, and
- pretend to be you to embarrass or misrepresent you, such as through social media.

Identity theft can be both financially and emotionally distressing for victims. Once your identity has been stolen it can be difficult to recover. You may have problems for years to come.

What can I do if I think I am a victim of identity theft?

If you think you are a victim of identity theft, it is important that you act quickly to limit the fraudulent use of your identity. You should report the incident to the ACORN, and take the following steps:

1. **Immediately inform the police**
   All incidents of identity theft should be reported to your local police (contact 131 444 or if you are in Victoria contact your local station) or through the ACORN. Ask for a copy of the police report or reference number because banks, financial institutions and government agencies may ask for it.
2. **Report the loss or theft of identity credentials to the issuing organisation**
   Contact the government or private sector agency which issued the identity credential if you have lost it or if it has been stolen.
3. **Alert your bank or financial institution**
   Contact your bank or financial institution immediately and cancel all cards and accounts that may have been breached.
4. **Get a copy of your credit report**
   Contact a credit reporting agency to check for unauthorised transactions. Make sure you can verify all 'inquiries' made into your credit history. Contact all companies and organisations that have made inquiries under your name that you did not authorise. Inform the credit reporting agencies that you are a victim of identity theft.
5. **Close all unauthorised accounts**
   Contact the credit providers and businesses with which any unauthorised accounts have been opened in your name. This may

include phone and utility providers, department stores and financial institutions. Inform them you have been a victim of identity theft and ask them to close the fraudulent accounts.

6. **Close any fraudulent or breached online accounts**
   Most websites, including social networking sites and online trading sites have a help section that contains specific advice about what to do if your account has been hacked or a fake account has been set up.

Please be aware that even if you follow all of the steps above, you may not be able to prevent unauthorised or fraudulent use of your identity. Further advice can be found in the Government's Protecting Your Identity pamphlet.

Case study

Michael from Alice Springs suspects that he is the victim of online identity theft. He receives an email from his bank, confirming that a new credit account has been opened in his name. The email contains the correct details of his full name, date of birth and bank account number, but incorrect details of his contact telephone number.

Michael should contact his email and social media providers, and his bank. He should also report this matter to the ACORN.