Identity theft

Do you know how to protect yourself?

What is identity theft?
Identity theft is a type of fraud. It involves stealing money or gaining other benefits by pretending to be someone else. Having your identity stolen can be devastating - both financially and emotionally.

Identity theft can occur in many ways. It may include someone using your credit card details illegally to make purchases or having your entire identity assumed by another person to open bank accounts, take out loans or conduct illegal business under your name.

How does identity theft work?

Identity theft works in a range of ways, from crude methods to well organised scams. Many of us have a wealth of personal information readily available such as cards in our wallet, mail, public records, information saved in our computers and information posted on social networking sites.

Identity theft **can happen easily and quickly.** Scammers will have easy access to your personal information if it is readily available. For example, scammers will pay people to rummage through rubbish tips and steal letters (also referred to as 'dumpster diving') to collect personal information. Blatant mailbox theft is also an ever-growing crime in many communities.

However, despite your best efforts, a determined scammer can also create elaborate and cunning plans to trick you into providing your personal details. For example:

Phishing scams are all about tricking you into handing over your personal and banking details. Most work by setting up special links in an email sent to you that take you to websites that look genuine.

Phoney fraud alerts are similar to phishing scams where scammers trick you into handing over your personal details. A common fraud alert involves the scammer pretending to be from your bank informing you that your credit card or account has been cancelled because of suspicious criminal activity. They will then trick you to provide account details to 'confirm' your identity.

Bogus job opportunities are usually posted on job websites. The scammer may use or sell your personal information provided in the job application.

The dangers lurking online[1]

Online identity theft may occur when personal information is used without your knowledge or permission. Personal information can be accessed from your computer or at a public computer terminal.

With sufficient information, criminals can use your information to:

- **open bank accounts** in your name
- **apply for credit cards or loans** in your name
- **transfer money** directly from your bank accounts
- **impersonate you online** on social networking sites.

Identity theft may damage your chances of applying for loans and credit cards.

How can you avoid it?

- Monitor your content. If you suspect your profile has been hacked, shut it down immediately.
- Use only websites with secure payment processes for online shopping and banking.
- NEVER post personal information. Small pieces of personal data can be used to build a much bigger picture.
- Change passwords. Passwords should be:
  - eight or more characters in length and include a combination of characters, numbers and symbols
  - changed regularly
  - never shared.

What can you do?[2]

- NEVER send money or give personal details to people you don't know and trust.
- Avoid getting phished. Don't respond to calls or emails from banks asking for passwords or other details. **A legitimate bank or financial institution will never email you asking for personal details or to follow a link.** If you receive a call from someone saying they're from the bank, ask for their name and a contact number or hang up and call back on their publicly listed number to see if it's authentic.
- Regularly check your credit card and bank statements to ensure that suspicious transactions are detected.

- Shred all documents containing personal information, such as credit card applications and bank statements.
- Search for and log directly on to a website that you are interested in rather than clicking on links provided in an email.
- Always seek independent advice if you are unsure whether an offer or request is genuine.

Other common scams

Credit card scams. There are many types that aim to steal your credit card details, either by taking the card itself or by tricking you into giving them the card details.

Card skimming. The illegal copying of information from the magnetic strip of a credit or ATM card can create a fake or 'cloned' card with your details on it.

Spyware and key-loggers. Spyware is a type of software that spies on what you do on your computer. Key-loggers record the keys you press on your keyboard. Scammers can use them to steal your online banking passwords or other personal information.

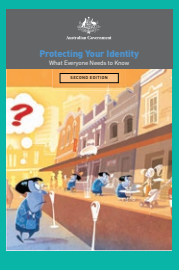
Work from home scams. These employment opportunities promise huge incomes with little work – usually by asking you to transfer money for someone else or recruit new victims. Remember – if it sounds too good to be true it nearly always is. And lastly…

Report them

If you think your identity has been misused, you should contact your financial institution to let them know. You can also **report a scam** to SCAMwatch.

Remember to tell your friends and family about the scam so they are alerted if they are targeted.

1. www.cybersmart.gov.au/Teens
2. www.scamwatch.gov.au/content/index.phtml/tag/identitytheft



Call the office for your copy of 'Protecting your identity - what everyone needs to know'.