Protecting Your Identity

What Everyone Needs to Know

Second Edition

Contents

Foreword

Your identity is one of the most valuable things you have. Being able to prove who you are is important for most aspects of your life – from getting a home loan to starting a new job to buying something online.

If criminals steal your identity, you may find everyday activities like these more difficult. The stress and financial costs can last for years.

The Australian government has published this booklet to help you protect your identity. It includes a number of quick and easy tips you can use to reduce the risk of becoming a victim of identity theft. You will also find suggestions about what you should do if your identity has been stolen.

You can never completely protect your personal information from falling into the wrong hands. However, if you follow the advice in this booklet you can significantly reduce the risk.

The Hon Mark Dreyfus QC MP
Attorney-General
Minister for Emergency Management

Summary

Protecting your identity can seem complicated, so here are 10 simple identity security tips:

1. Secure your personal documents at home, when you are travelling and if you need to destroy them.
2. Secure your computer and mobile phone with security software and strong passwords and avoid using public computers for sensitive activities.
3. Be cautious about using social media and limit the amount of personal information you publish online.
4. Secure your computer and mobile phone with security software and strong passwords and avoid using public computers for sensitive activities.
5. Learn how to avoid common scams at www.scamwatch.gov.au.
6. Be cautious about requests for your personal information over the internet, phone and in person in case it is a scam.
7. Investigate the arrival of new credit cards you didn't ask for or bills for goods and services that aren't yours.
8. Be alert for any unusual bank transactions or missing mail.
9. If you are a victim of identity theft – report it to the police and any relevant organisations.
10. Order a free copy of your credit report from a credit reporting agency on a regular basis, particularly if your identity has been stolen.

Why should I be concerned about identity theft?

Once your identity has been stolen it can be almost impossible to recover. You may have problems for years to come. Some of the things that criminals may be able to do with your identity include:

- tricking your bank or financial institution into giving them **access to your money** and other accounts
- opening new accounts and **accumulating large debts** in your name which will **ruin your credit rating** and good name
- taking 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
- **opening a phone, internet or other service account** in your name
- **claiming government benefits** in your name
- lodging **fraudulent claims for tax refunds** in your name and preventing you from being able to lodge your legitimate return

Peter was cleaned out by scammers*

"I was sick of my job so I put my professional details on a careers website. I was very excited when I got a call not long after from an overseas law firm offering me a job. The job sounded fantastic and best of all I would be moving overseas!

They needed to verify my identity so I emailed them a copy of my passport, payslip, bank account number and superannuation details.

The promised sign on bonus never landed in my bank. Instead they cleaned out everything I had from my bank and superannuation accounts.

I'm still trying to get my money back. My chances don't look good though because the money has gone overseas.

When I started investigating I found out that other people had been scammed in the same way. I really wish I had done a bit of research before sending them my personal details."

*Fictionalised example based on a real case

- using your name to plan or **commit criminal activity**, and
- pretending to be you to **embarrass or misrepresent you**, such as through social media.

How can my identity be stolen?

Through theft or loss of your personal documents

Personal information is information that can reasonably be used to identify a person. Your name and address are obvious examples. In some cases, your date of birth and post code may be enough to identify you. Personal information can also include your tax file number, bank account details, photographs, videos, and even information about your opinions and where you work – basically, any information where you are reasonably identifiable.

A personal document is any document that contains information about you. Examples include phone, bank and utility bills, medical records, tax refund assessment notices, home ownership deeds and rental agreements.

An **identity credential** is a type of personal document that is commonly requested by governments and businesses as evidence that you are who you say you are. It contains personal information about you, such as your name, date of birth, and address. Examples include your passport, birth certificate and driver licence.

Your identity may be stolen if:

- you lose your **purse, wallet or handbag** or it is stolen
- your home is broken into and **personal documents are stolen**
- thieves **steal mail** from your unsecured letter box, or
- thieves **retrieve mail, information or personal documents from your rubbish.**

Through theft of your personal information

Your identity can also be stolen if thieves gain access to your personal information. Even if you think thieves only have a small amount of information about you, they can use public sources like

social media to find out additional personal 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 credentials in your name or even apply for real identity credentials in your name, but with their photograph.

Your identity may be stolen if:

- you **provide personal information over the phone or internet** to what appears to be a legitimate business, but is actually a scam
- information about you stored on a business computer system is **illegally accessed by outsiders or corrupt employees**
- your **online account is hacked**
- your personal information is retrieved from **social media**, or
- **copies of your personal documents are stolen**.

Criminals used multiple sources to steal Jian's identity*

"In June I received a call from a very friendly man at the Australian Taxation Office (or so I thought) telling me that due to a change of legislation my last tax return had been reviewed and I was entitled to a refund. They knew a lot of information about me – like my name, address and date of birth – so I wasn't at all suspicious. All they wanted from me were some details from my last notice of assessment to check my identity.

He told me that it would take a few weeks to process the refund so I wasn't surprised that the money took a little while to land in my account. I first realised something was wrong when I tried to submit my tax return and received an error saying I had already submitted it! When I spoke to the tax office they told me they never called and it must have been a scammer.

Sorting the mess out has been a huge hassle. I've had to prove my identity to the tax office, apply for a new tax file number and have had to wait to receive my tax refund. They have also told me that my next year's return will be delayed until they make sure I was the one who lodged the return. I've also had to get a new bank account and change all my direct debits.

I still don't know how the scammers knew so much about me. I did hear on the news that putting your birthday and information about where you live on social networking sites can give scammers enough information to steal your identity. Maybe that's how it happened."

*Fictionalised example based on a real case

How can I protect my identity?

Protect your identity

Only carry essential personal documents

Try not to regularly carry important documents, such as your passport, outside of your home to reduce the risk of them being lost or stolen.

Destroy personal documents before putting them in the bin

Destroy important documents, such as bills, identity credentials and credit cards before you throw them out. Good ways to destroy documents include tearing, cutting, shredding or burning.

Sarah's personal information was used to make fraudulent claims*

"When my house was burgled I was so upset about the theft of my jewellery that I barely even thought about the fact that my passport, birth certificate and bills were stolen.

I sure remembered it though when Centrelink contacted me about the fraudulent welfare claims in my name!"

* Fictionalised example based on a real case

Make copies of key documents and keep them in a secure location

Make copies of your key identity credentials, such as your driver licence, birth certificate, or passport, and keep these copies in a secure location. The copies could be useful in re-issuing the originals if they go missing or are destroyed. They may also help you to verify your identity.

Protect your personal documents

Consider storing important documents and copies in a fire/water proof secure container or safe deposit box. Make sure documents stored electronically, such as copies of identity credentials, are secure. Strong passwords, encrypted files or trusted data vault websites are all options for secure electronic storage. Don't leave your personal documents in your car.

Secure your mail

Ensure you secure your letterbox or use a secure post office box. Remove mail from your mailbox as soon as possible. Only post mail at secure, official post boxes. Notify businesses and friends when you move house as soon as possible. Organisations you should inform include:

- banks
- credit and store-card companies
- utility providers
- your employer
- your accountant
- your university or school
- health care providers
- insurance companies, and
- sports clubs or gyms.

You should also inform any government agency you receive benefits from or deal with, such as the:

- Australian Taxation Office
- Department of Human Services (Centrelink and Medicare)
- Department of Veterans Affairs
- Australian Electoral Commission
- Roads agency in your State or Territory, and
- your local council.

Phoebe couldn't get a loan after her mail was stolen*

"I'm a student so I've moved around a lot and lived in a lot of share houses.

I'm pretty good at updating my address with businesses. I guess I must have forgotten to tell someone though because my identity was stolen.

I didn't even know it was stolen until I tried to get a phone on a contract. They told me I couldn't because of my poor credit history – even though I'd never had a loan before!"

* Fictionalised example based on a real case

Consider having your mail redirected for a few months after you move in case you forgot anyone.

Protect your documents when you are travelling

When you are travelling overseas take extra care of your personal documents. Make two photocopies of important documents, such as your passport, itinerary, visas, traveller's cheques, credit card numbers, driver licence and insurance policy. Leave one copy at home with your family or a friend and the other separate from the originals in a safe place while you're travelling.

Treat any request for personal information or copies of your identity credentials with caution

Ask businesses why they are collecting your personal information, how it will be used and stored and who the information will be passed on to. Read the company's privacy policy and if you don't agree with it, don't do business with them. Consider selecting the 'opt out' box on forms.

There are certain industries, such as the financial and telecommunications industries that have a legal requirement to verify your identity before they provide a service. For example, the Australian Government introduced the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* to prevent money-laundering and the financing of terrorism. The Act applies to all entities that provide financial services, such as your bank or credit union. A key element of the Act is that businesses know who their customers are. This means that they are legally obliged to ask you to provide evidence of your identity.

An industry code of conduct that includes basic identity checks may be sanctioned by a Commonwealth, State or Territory government. Codes of conduct are often designed to allow industries to quickly respond to changing circumstances, something that can be difficult to achieve in a legislative regime. If you are asked for information and you are told that it is under a code of conduct or practice, you can ask where to find official government information about it before deciding whether to comply with any request for personal information.

Limit the information contained in family trees

Limit the amount of information about living individuals on family trees – particularly if it is online. Information commonly included on family trees, such as name, date and place of birth and mother's maiden name could be used to commit identity theft.

Order a copy of your credit report annually

Check your credit report annually to catch any unauthorised activity. Credit reports can be ordered from one of the three main credit reporting agencies in Australia (listed on p16). Consider asking for an alert to be placed on your file so you are notified of requests for finance that haven't come from you.

Check your banking and superannuation records carefully

Check all transactions on your banking, credit card and superannuation accounts regularly. You

Priya and Helen weren't suspicious of a recommendation from a friend*

Jen, Priya and Helen had been planning a trip to South America for months. Priya and Helen were very excited when Jen sent them a link via social media to a competition that had a prize of an all-expenses paid holiday. It was exactly what they were after!

All Priya and Helen had to do was enter a few personal details, like their name, address and driver licence number to make sure that they weren't entering the competition multiple times.

Unfortunately when they spoke to Jen she had no idea what they were talking about. A scammer must have hacked into her account and sent them the links.

Priya and Helen have no idea who has their personal information or what they will do with it. They've reported the theft to Scamwatch, the police and set up an alert with a credit reporting agency in case they apply for credit in their name and are hoping this will be enough to catch anyone trying to use their personal information.

may be able to detect potential identity theft early and limit the damage.

Protect your identity online

Protect your computer

Criminals are constantly developing new viruses and programs to steal or access your personal information. To help secure your computer from unauthorised access you need reputable security software. The security software package should include virus, malware and spyware protection and a firewall. If you're not sure what software is reputable, ask at your local computer store, look through IT magazines or online surveys of security software. Make sure the security software is set to update automatically and that you regularly scan your computer's files. Ensure you renew your security software when the subscription is due.

Avoid entering personal information or a password on an unsecured website

The address of secure websites, such as online banking, will start with 'https' or have the 'closed padlock' symbol displayed.

Use passwords and access controls

Protect your computer and important documents with passwords and access controls. This is particularly important if you have a wireless network. Ensure you change your passwords regularly and that they contain a mixture of upper and lower case letters, numbers and other characters. Strong passwords which are unique and unpredictable are less likely to be cracked.

Protect your passwords

Try to memorise your passwords and personal identification number (PIN), store them in a safe place or use password management software. Don't write your passwords down and leave them in an obvious place, such as your wallet or in a file on your computer. Don't share them with

friends or family. Never select the option ‘would you like the computer to remember this password’ when logging onto a site.

Use different passwords and usernames

Use different passwords and usernames for different sites, particularly those for sensitive transactions such as banking. Even if one account is compromised the others won’t be vulnerable to hacking.

Never click on a link or open an attachment in an e-mail from someone you don’t know and trust

Avoid opening attachments or clicking on links in e-mails, unless you trust the email source. Attachments and links can download malicious software into your computer or can redirect you to a fake site. It is much safer to type in the web address yourself than to follow a link.

If you receive an email asking for personal details from what looks like a trusted source, don’t hit ‘reply’ – it could be a scam that is impersonating the trusted source. Answer with a new email message using an email address that you have safely used before or trust. Consider contacting the sender to check if the request is legitimate.

Social networking safely

Criminals can use information on social networking sites to steal your identity. Make sure you set your social network profile to ‘private’. Be cautious about which ‘friend’ requests you accept. Ideally you should only accept ‘friend’ requests from people you’ve met in real life. Think before you post – expect that people other than your friends can see the information you post online. Don’t post information that would make you or your family vulnerable – such as photographs, your date of birth, address, information about your daily routine, holiday plans, or your children’s schools.

Avoid using public computers to access your personal information

Personal information, like passwords, can be retrieved from a computer's hard drive. Limit your use of public computers for sensitive transactions, such as accessing email accounts. If you do use a public computer, check to see if the service provider has any security settings. Always remember to clear the history and close the web browser before you leave the terminal.

Safe computer disposal

Make sure no personal information is left on your computer when you sell or dispose of it. Deleted files can sometimes be recovered so you should consider using 'data destruction' software.

Protect information on mobile phones

Information stored on mobile or wireless devices is at risk of physical or electronic theft. Limit the personal details stored on mobile phones or wireless devices. Use a password or PIN. Turn off wireless features when you aren't using them and only connect to secure (encrypted) wireless networks. Only download applications from official stores or trusted sources. Smartphones are susceptible to malicious software attacks so consider anti-virus software for your phone.

Mobile phone disposal

Make sure no personal information is left on your phone when you dispose of it. Check with your telephone's manufacturer for instructions on how to delete information.

Protect yourself from scams

Ask questions and be suspicious

If an offer sounds too good to be true, it probably is. Be wary of ads posted on the internet, like job ads on social networking sites. Be cautious if you've won a lottery you never entered. Ask questions if you have concerns. Don't agree to anything straight away. If you think the offer is legitimate, carry out some independent research before committing yourself.

Online dating safely

Identity thieves can use dating websites to steal information from you. If someone asks you for bank or personal details, money or gifts you should always exercise caution and consider the possibility that it may be a scam, even if you think you know the person well.

Simon was fooled by a beautiful woman*

"I was sceptical of dating websites so wanted to take things slowly with Danielle, but over the months we gradually got closer. She didn't have a video camera, but she sent me photos. She sure was stunning!

When Danielle told me her mother was sick and she couldn't afford to pay the medical fees, I didn't hesitate to send her the $20,000 she needed.

I never heard from her again. Worse still, she used the personal details I'd told her, like my name, date of birth and place of birth, to steal my identity. I found this out after the police contacted me about a credit card in my name that was being used for illegal activities."

* Fictionalised example based on a real case

Social networking scams

If you receive an unusual request from a friend check directly with the friend and do some research to confirm it is legitimate. Beware of scams on social networking sites, such as expensive gifts in exchange for filling out a survey. The survey could be used by scammers to collect your personal information and you may never receive the gift. They could also use it to hijack your account and spam your friends.

Avoid giving personal or financial information over the phone

If you receive an unsolicited phone call from someone wanting to know your personal details—hang up. Banks and financial institutions may contact you if there is suspected fraudulent activity with your account. If you do need to provide personal information over the phone, hang up and contact the organisation through the advertised number on their website or in the phone directory.

Do not allow remote access to your computer

If you receive an unsolicited call from an internet service provider, telecommunications company or software provider, do not give them remote access to your computer. Remote access gives identity thieves unlimited access to steal any personal information you have stored on your computer, such as copies of identity credentials and photographs.

Contact the Do Not Call Register

The Do Not Call Register allows individuals to register if they do not want to receive certain unsolicited telemarketing calls. Register via the website www.donotcall.gov.au or by phoning 1300 792 958.

Ruth's personal details were stolen after scammers gained access to her computer*

"I'm not very tech savvy so just ignore any error messages that pop up on my computer. I wasn't surprised then when someone from my software company called me. They said that my computer had sent them an error message and they needed to log onto my computer to investigate it.

After logging onto my computer they said it had a virus that would need to be removed. I didn't want a virus so paid them the $99 to clean up my computer. I went away to make lunch while they were cleaning my computer because they said it would take about an hour.

My husband was horrified when he found out what I had done. He said it was probably a scam.

When I took my computer into an IT shop they said that there was now software on the computer that could be used to remotely control my computer.

The scammers also used copies of identity credentials I had on my computer to try to apply for a credit card. Luckily I had called a credit reporting agency and put an alert on my file so I was able to stop this happening."

* Fictionalised example based on a real case

How will I know if I'm a victim of identity theft?

You may not even know you are a victim of identity theft until long after it has happened. You should look for these warning signs:

- **calls from creditors, debt collectors or solicitors** about transactions you didn't enter into or debts that aren't yours
- arrival of **new credit cards** that you didn't ask for
- unexpected **denial of credit**
- **refusal of services or benefits** because you are told you are already receiving them
- mail you were expecting, such as bills, not arriving or a **reduction in mail**
- **arrival of bills for goods or services you didn't order**
- unfamiliar **charges or withdrawals** on your credit or bank card, or
- **lost wallet, purse or identity credentials** – even if you lose them and they are returned they could have been copied.

Sharing passwords is a risk Andrew won't take any more*

"I lent my laptop to my mate Danny so obviously I gave him the password to log in. He must have been bored one afternoon because he decided to see if he could use it to log onto my Facebook account.

He just made a few silly posts from my account – nothing that caused any problems. It was a real wakeup call though! I now have different passwords for all my accounts and certainly don't share them with anyone.

* Fictionalised example based on a real case

What should I do if I'm a victim of identity theft?

If you suspect you are a victim of identity theft you should take the following steps to minimise any financial or other damages. The quicker you act, the more likely you are to avoid problems. However, even if you do follow all these steps you may not be able to prevent unauthorised or fraudulent use of your identity.

1. Immediately inform the police

All incidents of identity theft should be reported to your local police (listed on page 14). Ask for a copy of the police report or a crime 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 who issued the identity credential if you have lost it or if it has been stolen (key agencies listed on pages 14 - 15).

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 (listed on page 16) to check for unauthorised transactions. It is advisable to check your credit report at least once per year. 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. Consider asking for an alert to be placed on your file so you are notified of requests for finance that haven't come from you.

5. Close all unauthorised accounts

Contact the credit providers and businesses with whom 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 online sites, such as social networking or email providers have a help section. These sections generally contain specific advice about what to do if your account has been hacked or a fake account has been set up.

7. Check that your mail hasn't been redirected or address changed

Contact Australia Post to check a redirect hasn't been placed on your mail (listed on page 16). You should also check with businesses and government agencies you deal with that your address hasn't been changed.

8. Contact the Office of the Australian Information Commissioner if you feel your privacy has been breached

You can contact the Office of the Australian Information Commissioner if you feel your privacy has been breached (listed on page 16). Their Enquiries Line is available to help you work out if a privacy breach may have occurred. Before lodging a complaint with the Office of the Australian Information Commissioner, try to resolve matters with the agency or organisation concerned.

9. Investigate whether a Commonwealth Victims' Certificate may help you restore your identity

If you are a victim of a Commonwealth identity crime and the theft is causing you problems in your business or personal affairs you may find a Victims' Certificate helpful. Examples of Commonwealth identity crimes include use of your personal information to falsely claim a benefit from Centrelink, submit a false tax return or purchase and import illegal substances. The Victims' Certificate is provided by a State or Territory magistrate. You can present it to government agencies or businesses, such as credit reporting agencies, to help support your claim that you have been a victim of a Commonwealth identity crime. To find out if you are eligible and how to apply please visit www.ag.gov.au/identitysecurity or contact CriminalLaw@ag.gov.au.

Whom should I contact?

Police

ALL STATES AND TERRITORIES (EXCEPT VICTORIA)

☎ 131 444

VICTORIA

☎ (03) 9247 6666

www.police.vic.gov.au

NEW SOUTH WALES

www.police.nsw.gov.au

QUEENSLAND

www.police.qld.gov.au

WESTERN AUSTRALIA

www.police.wa.gov.au

SOUTH AUSTRALIA

www.sapolice.sa.gov.au

TASMANIA

www.police.tas.gov.au

NORTHERN TERRITORY

www.pfes.nt.gov.au

AUSTRALIAN FEDERAL POLICE (ACT POLICING)

www.afp.gov.au

CRIME STOPPERS

☎ 1800 333 000

www.crimestoppers.com.au

Lost or stolen citizenship certificate, visa or other immigration document

DEPARTMENT OF IMMIGRATION & CITIZENSHIP

☎ 131 881

www.immi.gov.au

Lost or stolen Medicare card

DEPARTMENT OF HUMAN SERVICES (MEDICARE AUSTRALIA)

☎ 132 011

www.humanservices.gov.au

Lost or stolen driver licence

Contact the relevant Road Authority that issued your licence:

NEW SOUTH WALES

☎ 132 213

www.rms.nsw.gov.au

VICTORIA

☎ 131 171

www.vicroads.vic.gov.au

QUEENSLAND

☎ 132 380

www.tmr.qld.gov.au

WESTERN AUSTRALIA

☎ 131 156

www.transport.wa.gov.au

SOUTH AUSTRALIA

☎ 131 084

www.transport.sa.gov.au

TASMANIA

☎ 1300 851 225

www.transport.tas.gov.au

AUSTRALIAN CAPITAL TERRITORY

☎ 132 281

www.rego.act.gov.au

NORTHERN TERRITORY

☎ 1300 654 628

www.nt.gov.au/transport

Lost or stolen birth, marriage, death or change of name certificate

Contact the relevant Registrar of Births, Deaths and Marriages that issued your certificate:

NEW SOUTH WALES

☎ 1300 655 236

www.bdm.nsw.gov.au

VICTORIA

☎ 1300 369 367

www.bdm.vic.gov.au

QUEENSLAND

☎ 1300 366 430

www.justice.qld.gov.au/bdm

WESTERN AUSTRALIA

☎ 1300 305 021

www.bdm.dotag.wa.gov.au

SOUTH AUSTRALIA

☎ 131 882

www.ocba.sa.gov.au/bdm

TASMANIA

☎ 1300 135 513

www.justice.tas.gov.au

AUSTRALIAN CAPITAL TERRITORY

☎ (02) 6207 3000

www.ors.act.gov.au

NORTHERN TERRITORY

☎ (08) 8999 6119

www.nt.gov.au/justice/bdm

Lost or stolen passport

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE

If your passport is lost or stolen within Australia:

☎ 131 232

www.passports.gov.au

If your passport is lost or stolen whilst you are overseas, report the loss to the nearest Australian diplomatic or consular mission. A list of Australians missions is available at:

www.dfat.gov.au/missions

Lost or stolen foreign documents

If you have lost vital documents, such as a foreign passport not issued by an Australian government agency, then contact the relevant diplomatic or consular mission. A list of foreign missions is available at:

http://protocol.dfat.gov.au/Mission/list.rails

Credit reporting agencies

You could have a credit report with more than one reporting agency. If you live in Tasmania you may need to check with the Tasmanian Collection Agency and Veda Advantage. If you live in other states you may need to check with Veda Advantage and Dun and Bradstreet.

VEDA ADVANTAGE

☎ 1300 762 207

www.mycreditfile.com.au

DUN AND BRADSTREET (AUSTRALIA) PTY LTD

☎ 132 333

www.dnb.com.au

TASMANIAN COLLECTION SERVICE

Tasmanian residents

☎ (03) 6213 5555

www.tascol.com.au

Other important contacts

AUSTRALIA POST

☎ 137 678

www.auspost.com.au

DEPARTMENT OF HUMAN SERIVCES (CENTRELINK)

Fraud Tip-off Line

☎ 131 524

Report a suspected fraud online:

www.humanservices.gov.au

AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Scamwatch

☎ 1300 795 995

www.scamwatch.gov.au

AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY

Spam emails can be forwarded to report@submit.spam.acma.gov.au
Spam SMS can be forwarded to 0429 999 888

www.spam.acma.gov.au

AUSTRALIAN TAXATION OFFICE

Lost or stolen tax file number or other tax documents

☎ 132 861

www.ato.gov.au/identitysupport

AUSTRALIAN SECURITIES & INVESTMENT COMMISSION

☎ 1300 300 630

www.asic.gov.au

OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

☎ 1300 363 992

www.oaic.gov.au

Use this space to list any other important contacts, such as your bank or mobile phone provider.

Organisation:

☎

Organisation:

☎

Organisation:

☎

Organisation:

☎

Organisation:

Where can I go for more information?

Identity security

www.ag.gov.au/identitysecurity – for individuals and businesses

Financial identity security

www.moneysmart.gov.au – for individuals and businesses

www.protectfinancialid.org.au – for individuals and businesses

Cyber security

www.staysmartonline.gov.au – for individuals and small business

www.cert.gov.au – for large businesses

www.cybersmart.gov.au – for children, parents and teachers

www.ag.gov.au/cybersecurity – for information on government policy

www.icode.net.au - Internet Industry Association's voluntary code of practice on cyber security

Privacy

www.oaic.gov.au – for individuals and businesses

Scams and fraud

www.scamwatch.gov.au – for individuals and businesses

Identity security checklist

How vulnerable are you?

PERSONAL SECURITY	**YES/NO**
Do you let your credit card out of your sight when paying a bill?	
Do you leave your personal documents lying around your home or office unsecured?	
Do you have your mail delivered to an unlocked home letterbox?	
Do you leave any personal papers in your car's glove box?	
Do you put sensitive papers in your household recycling or garbage bin?	
Is it more than a year since you have checked your credit report?	
COMPUTER SECURITY	**YES/NO**
Do you forget to regularly change your passwords?	
Do you keep personal information on your computer?	
Is your virus protection software out of date?	
Is it more than a fortnight since you have scanned your computer for viruses?	
Do you not have personal firewall protection?	
Do you use a wireless internet connection without protecting it with a password?	
Do you use public access computers?	
Do you post personal information on a social networking site?	

The greater the number of 'yes' responses, the more vulnerable you are to become a victim of identity theft.

Additional electronic copies of this booklet are available from the Attorney-General's Department website www.ag.gov.au/identitysecurity.

ISBN:

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour (http://www.itsanhonour.gov.au) website.

Contact Us

Inquiries regarding the licence and any use of this document are welcome at:
Business and Information Law Branch
Attorney General's Department
3-5 National Circuit
Barton ACT 2600
Telephone: (02) 6141 6666
copyright@ag.gov.au