How safe is your identity?

Advances in technology are making identity fraud one of the fastest growing crimes in Australia, but 75%* of Australians continue to put themselves at risk by not taking simple precautions.

What's identity fraud?

Identity fraud occurs when a person uses a stolen identity to obtain credit, goods or other services fraudulently. This can happen if the person acquires sensitive information, such as credit card details, date of birth, mother's maiden name or passwords.

Typical tactics

Criminals use various tactics to acquire the information they need to steal your identity, such as:

+ stealing information provided on unsecured websites
+ redirecting your mail to another address or stealing mail, such as super statements, from mailboxes
+ phishing, which is stealing information using email. See over page for more information
+ stealing your wallet, purse or mobile phone
+ phone calls claiming to be from a bank asking you to update your personal information
+ raiding your rubbish bin for credit card statements, tax information, old bills, insurance documents and bank statements
+ card skimming, which occurs when a shop assistant or waiter copies your credit card details when you make a purchase
+ offering to complete your tax return or other documents containing personal information.

ⓘ If you're a victim of fraud call the police and notify your bank.

Safety checklist

Important documents

+ Check your bank, credit card and super account statements for suspicious transactions.
+ Shred any documents with sensitive information, such as bills, bank statements, expired credit cards and compact disks before throwing them out.
+ Store important information, such as passports and marriage certificates, in a locked cabinet.

Your purse or wallet

+ Don't carry sensitive information, such as your tax file number, birth certificate or PIN number in your purse or wallet.

Your mail

+ Avoid including personal details, such as your tax file number, on documents sent by post.
+ Lock your mailbox to keep it secure.
+ Redirect mail with Australia Post if moving house.

Your computer and mobile phone

+ Don't keep sensitive financial information online, on a computer or mobile phone.
+ Use a pin to secure your mobile phone.
+ When shopping online, make sure there is a secure connection (https) by looking at the address bar or checking for the 'lock' symbol.
+ Limit the information you put on social networking sites and use the privacy tools available.
+ Avoid sending personal information via email.
+ Install up-to-date anti-virus, anti-spyware and firewall software.
+ Only download apps from reputable publishers and check the permission requests.

Dealing with organisations

+ Only provide identity details to trusted organisations.
+ Only offer credit card details over the phone if you initiate the call.
+ Only deal with registered tax agents to complete your tax return.

*Galaxy Research Omnibus (May 2007)

Staying smart online

The internet is a popular and convenient way to shop, bank and carry out other business. Unfortunately, some people exploit users by tricking them into revealing personal information, such as usernames, passwords and credit card details.

This is known as 'phishing'. Pronounced 'fishing', the term relates to the baits used to 'catch' financial information and passwords.

Phishing emails often look authentic and purport to be from a trustworthy source. For instance, you may receive an email from someone masquerading as your bank. While the email may use the names of real people, have the right logos and fine print, they give themselves away by asking you to provide your personal details via a reply email or website.

Taking precautions against phishing

While it's natural to be alarmed by an email claiming your account is frozen or your credit card information was stolen, resist your first impulse to reply and take some simple precautions.

- Remember, legitimate companies never ask for your account details or passwords through email. If you receive such a request, it's almost certainly a scam.
- If you receive an email asking for personal information and you want to contact the company to check if it's legitimate, use the phone number listed in the phonebook, not the one in the email. The phone number may be false or lead to you incurring costs.
- Likewise, follow your own path to the website instead of trusting the hyperlink provided in a suspected phishing email. Do this by typing the company's genuine address into your browser's address bar.
- Report the suspect email to the institution concerned. If there's a chance of fraud, report the crime to the police in your State or Territory.
- Delete the phishing mail, as it may carry viruses. Never click on attachments.
- Secure your computer by running and maintaining an anti-virus product, not running or installing programs of unknown origin and using a personal firewall.

Quick quiz – would you get caught?

1. You receive an email from your bank saying your credit card contains some irregular transactions and you need to provide your credit card details via return email for the claim to be investigated.

2. You receive an email from your financial institution stating a recent security upgrade means you have to log on to your account to be protected.

3. You receive an email from a company stating your account will be closed unless you log on with your username and password.

Mine Super will never ask for your personal information via email

We're serious about protecting your information. That's why we'll never send you an email asking you to verify your personal information or provide your password, member number or other account details.

If you do receive such an email we recommend you don't respond to it under any circumstances and forward the email in its entirety to webmaster@mine.com.au then delete it.

Where can I find more information?

For more information about scams, visit the government's MoneySmart website at moneysmart.gov.au/scams

You can also speak to our service officers on 13 MINE (13 64 63), Monday to Friday, 8am to 6pm or email help@mine.com.au

01-01-03-039/CAN171253a/J5008/010718