

private i

Your ultimate privacy survival guide



Privacy is everybody's business

How often do you think about your privacy when doing any of the following everyday things...?

Using social networking sites

Do you ever stop to think about who'll be looking at the information you post?

Getting your ID scanned at bars and clubs

Do you wonder what's going to be done with your digitised information?

Filling in a form

Do you ever read the fine print?

Shopping or banking online

Do you check the system is secure before providing account or credit card details?

Receiving junk mail, spam or telemarketing calls

Do you ask yourself how they got your details and how to get them to stop sending you stuff?

You probably don't realise just how many decisions you make about your privacy every day. These decisions are your choices – you have the power to make the best privacy choices in a way that works for you.

Whether you never think about privacy or always do, this publication is for you. It'll tell you what some of the privacy issues are that you may face, some of the pitfalls to avoid, and who to turn to for help if your privacy has been affected.

BUT... and yes, there is a but: This publication is only a few pages long and there's so much more to be said about privacy issues. So, if you need any further information, visit us at www.privacy.gov.au, or give us a call on 1300 363 992.

QUIZ:

How much information do you give away?

You're going to a club or bar and the bouncers ask for your driver's licence to scan, or they want to scan your fingerprints. Do you:

- a.** Happily present your card and your fingertips and thank your lucky stars that the photo of you is a good one and that you just did your nails?
- b.** Politely tell the bouncers to "go scan yourselves" and see how they react...?
- c.** Ask to read their privacy notice? If you can't see one you ask the bouncers why they are being scanned and what will be done with the digital images.

You're updating your profile on Facebook, MySpace, Twitter or another social networking site. Do you:

- a.** Post whatever you want (it's only a forum for your friends after all...)?
- b.** Try to be selective in what you post about yourself or others (such as nothing you'd be embarrassed for your grandparents to see)?
- c.** Only post non-identifying information (leaving out your contact details, date of birth, etc.)?

You are invited to enter a competition to win a trip to Thailand. Do you:

- a.** Enter the competition and provide whatever personal details they ask for on the form? (After all, it's the price you pay to win a free holiday.)
- b.** Glance at the competition's privacy notice and, if it basically looks okay, enter the competition? (You should always look at how your privacy will be safeguarded.)
- c.** Read the privacy notice in detail and, only if you are satisfied with it, complete the form, providing the least amount of personal information possible? (You can never be too trusting about your privacy.)

Your friend doesn't have a credit card and wants to borrow yours so they can buy something online. Would you email your friend your credit card details?

- a.** Yes. (Who cares about ID theft? Good luck to anyone who thinks they can get their hands on your non-existent 'millions' by stealing your details.)
- b.** Sometimes. (You try to encrypt emails with important information, or to call the person with the details, but every now and again you risk it.)
- c.** Never. (You're asking for trouble by including personal information in an email. It doesn't take much for scammers to get hold of your details.)

How often do you read a business's privacy policy or ask what will be done with your personal information that they are collecting?

- a.** Never. (Come on, businesses are going to safeguard the personal information they hold about you. It's the law, isn't it?)
- b.** Sometimes. (Only when the business collecting your information doesn't look legit.)
- c.** Always. (You can never be too cautious.)





how you rated

Mostly “a”s:

Privacy risk taker. You’ve been using a computer since you were five and nothing bad has ever happened, so you think: “Why should I start worrying about privacy issues after all this time?”. Right? Wrong! Your blasé attitude to protecting your personal information even has some of your friends on edge. Most of them wouldn’t trust you with their personal details if it came down to it. It’s time to take control of your privacy and stop giving out your personal information. After all, privacy is one of those things that you only really value when it’s gone. Go on, take control now!

Mostly “b”s:

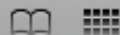
Relaxed for better or worse. Let’s face it – when it comes to privacy you’re not bad, maybe even pretty good. You usually read privacy policies and you think before you post on Facebook that hilarious photo of you at a party dancing in fairy wings. But how often do you actually take action based on your intuitions about privacy? Not often enough, it seems. Trust your intuitions – if a website or competition looks dodgy, then it probably is. If you’re sending credit card details by email, use encryption. It’s great to be relaxed when managing your personal information – but imagine how much better things could be if you went the extra mile!

Mostly “c”s:

Privacy defender. Privacy is important to you. You’re not about to let someone mess around in your personal affairs. It’s not that you’re uptight about it. You’d just prefer to know that your anti-virus is up-to-date, your passwords are secure (and not scrawled on a scrap of paper) and your personal information is only held by those you trust. All of this means that you sleep pretty well at night. And why wouldn’t you? You have control over your information and no one’s gonna take it from you without a fight!



http:// social networking online/



Social networking sites like Facebook, MySpace, Twitter, Friendster and Bebo can be great fun. There is nothing more entertaining than checking out photos of the weekend, laughing at people's comments and keeping a general eye on what's going on with your mates.

But, like everything in life, social networking sites come with some risks – what you post on them could impact on your privacy.

Take these examples:

- You figure it can't hurt to put some information about yourself in your online profile, such as your date of birth and a photo. However, you don't realise that you've mistakenly added as a "friend" to your page someone who is anything but... they're really a cybercrim who pieces together the information in your profile and other things about you online to apply for a credit card in your name and to pretend to be you...
- Your profile (or your friends') includes photos of you in various poses after a wild night out. Your partner was out of town that night and gets quite a shock when they see what you've been up to in their absence.
- You leave a message on your page on the site saying that you're calling in sick to work so you can go to the beach. It just so happens that some of your work mates have access to your page and tell your boss. You're in for a nasty shock from your boss when you return to work tomorrow.
- You want to invite some people over for some drinks and you post an invite on your page on the site, thinking only your closest friends will pay any notice to it. What you didn't expect is so many of your

'friends' who have access to your page to gatecrash.

- You take some photos of your friend while they're 'off their face' with your mobile and post these on your page for everyone to see. It may be hilarious now, but think of what'll happen if your friend's parents, partner or work colleagues get hold of them?

We are all going to continue to use these sites, so be smart about the way you use them. Think twice before you upload!

Questions about privacy and social networking? Check out some FAQs and a video at www.privacy.gov.au.

What you can do

Read the privacy policy of the social networking site

Be careful about what information you give out about yourself or others

Use the privacy tools available

Make sure your anti-virus software is up-to-date



What makes you you?

It's a deep philosophical question, you may say, and you'd be right. But that's not all it is – it also has practical ramifications, and sometimes very worrying ones.

Think about it. With just a handful of details, others could pretend to be you.

Of course, sometimes it's nice to think that others want to be like you, copying your sense of fashion, envying your taste in music, or admiring your sporting achievements. But it's not so nice, to put it mildly, when those wanting to be like you are out to steal your identity.

It's become one of the world's pervasive crimes of the 21st Century, and Australia is no exception. A 2007 survey by the Australian Bureau of Statistics found that nearly one billion dollars had been lost as a result of personal fraud.

Frank Abagnale, the inspiration behind the Spielberg movie, *Catch Me If You Can*, became infamous as America's most gifted con man. Abagnale spent his late teens and early 20s ripping off everyone he could until, following time served in jails in France, Sweden and the US, he switched sides and has spent the past three decades speaking out about identity theft. One of his observations is particularly worrying, "What I did 30 years ago, is 200 times easier to do today than it was then, and five years from now will be 700 times easier than it is today".

Technology has made life much easier for ID thieves. Not only is the personal information of so many people available for the taking online, but creating forged documents or fraudulently applying for credit can also be done electronically with comparative ease.

Sometimes all it takes are some basic facts about you for your identity to be stolen, such as your name, address, date of birth, bank account and credit card numbers, or passwords. Knowing even a few of these things could be all that's needed for someone else to open up a line of credit in your name and spend like there's no tomorrow.

"About six months ago I received a letter saying that I had totally maxed out the \$4,000 limit on my credit card. This simply wasn't possible.

"The credit card company said they had a record of my calling them saying I had supposedly lost my card. The caller was able to provide my date of birth, mother's maiden name, phone number and address. They must have guessed that I had a certain type of credit card, called up the company, said they were me and had lost the card. They probably said they couldn't remember the card number, but were able to 'prove' they were legit because they had all these other details.

"Anyway, the person got sent a 'replacement' card in my name, and then they maxed it out pretty rapidly.

"Thankfully the card company covered the fraud, but I had an awful time proving that the replacement card was sent to someone else, not me, and that I was the victim of ID theft.

"I suppose the person got my details from the web. Anyone who goes looking could probably find out the basics about me.

"Anyway, dealing with all of this is not something I'd ever want to go through again, that's for sure."

- Mark C.

ID theft prevention

- If an organisation or person wants to collect personal information from you, ask why the information is required, what they will do with it and who will it be disclosed to. Only give out as much personal information as you need to.
- Think twice before posting any personal information about yourself online.
- Install anti-virus and anti-spy software on your computer, as well as firewalls.
- Regularly check your credit card and bank statements for suspicious transactions.
- Minimise the amount of personal information you carry around, especially at places where it is likely to get lost or stolen, such as the beach, club, etc.
- Shred all documents you no longer need that contain personal information. (A 2007 survey found that 75% of Australians throw out enough personal information in their rubbish and recycling to put them at risk of identity theft.)
- Use the privacy settings on social networking sites.
- Watch out for scams!
- Monitor your credit report – see www.mycreditfile.com.au
www.dnb.com.au
www.tascol.com.au

More information

www.scamwatch.gov.au
www.staysmartonline.gov.au



ID Scanning

Having people glance at our ID is something we are all used to. It happens all the time – when you enter a club, buy alcohol or join a video store. Most of us don't really have an issue with that. Someone checks that it is you, looks at your date of birth, and assuming all is above board, off you go for a good night out.

However, there's another step to this process that's becoming more and more routine – ID scanning.

ID scanning is when a business uses equipment to take an electronic copy of your ID. Pub and club owners do this primarily so they know who is in their club on a certain night, therefore making it easier for them to pinpoint people who may have caused trouble.

So, I guess we all think - what's the problem with that?

Once your ID has been scanned, your personal information contained on the ID is digitised and stored by the business. Depending on the privacy practises of that business, your information could then be used or disclosed for many other purposes than simply identifying who was in the club that night. The business may use or pass on your information for direct marketing, or match it with information about you held by other businesses. This could create a very detailed picture of how you go about your daily activities.

With the prevalence of identity crime, what information businesses and their staff have about you is something you may want to think about.

So, next time a business asks to scan your ID, ask them why they are collecting that information, how they plan to use it, who has access, and how long the information will be kept.

For more information about privacy and ID scanning, visit: www.privacy.gov.au





Dealing with telemarketers

It isn't always so pleasant being on the receiving end of telemarketing calls, especially when you've just got home and are preparing dinner. While telling telemarketers where to go or hanging up the phone is one way to get rid of them, there's a better way... add your number to the Do Not Call Register (www.donotcall.gov.au). It doesn't stop market researchers and charities from calling you, but at least it'll give you some peace and quiet from people trying to sell you things.

Why do you want to know?

From credit card or car loan applications to Centrelink payments and Medicare claims, it can be really annoying having to provide information about yourself and your finances time and time again. This information may be needed by the organisation so they can provide you with a service, but it's important to know why the organisation is collecting the information and what will be done with it.

If you don't understand why a particular piece of information is being collected or you want to know that your personal information will be stored securely and destroyed when no longer needed, then follow this simple advice: ASK! It's your information and you have every right to want to protect it, so ask the organisation. If you're not happy with the answers and believe that they aren't doing the right thing under the Privacy Act, see www.privacy.gov.au or call 1300 363 992 for advice about the Office of the Privacy Commissioner's complaints process.



“To buy or not to buy, that is the question”

The beauty of online shopping (aside from the fact that it's convenient) lies in our new found ability to shop worldwide and only have to lift a finger. With a few simple clicks we can pick the newest and hottest item of our desire, enter our credit card details and personal information and voila, in no time at all the goods are literally at our doorstep.

It almost sounds too good to be true – and sometimes it is.

When shopping online you really should make privacy and security your number one priority. There are easy ways you can do this, the most obvious are:

- ✓ check you are shopping on a secure website (look for the 'lock' symbol)
- ✓ read the privacy notice to find out how your personal information will be used. Is the hottest pair of shoes really worth non-stop spam?
- ✓ trust your instinct – if you're not sure about the safety of a site or you don't feel comfortable with how your personal information will be used, think twice.

It's your personal information and it's up to you to protect it.

For tips on how to safeguard your privacy online, visit www.staysmartonline.gov.au.

Your health information

Did you know that the Privacy Act gives you a right to access your medical records (and that in general, no one else can access them without your permission)?

And did you know that health services and other businesses generally need your consent to collect your health information?

The Office of the Privacy Commissioner has a range of FAQs to help you understand your health privacy rights: www.privacy.gov.au.



When black is not the new black

You know the feeling – you get your credit card bill and it's massive. Suddenly, you realise that buying your friends that round of drinks at the bar wasn't such a good idea. Oh well – you'll just be a little bit late with the payment, no real harm.

Or, you've changed your mobile phone service provider because of a great new offer, but you don't pay the last bill with the old company. After all, it's only a few hundred dollars and you're never going to use that company again.

Or, you're about to move in with friends and you just can't wait to get out of the place you're in that you don't bother giving it a proper end of lease clean. You know you should be leaving the place clean, but there's nothing the estate agent can do about it, is there? Worst case scenario – they'll just keep your bond, right?

WRONG.

The reality is that your name could end up on a 'blacklist'. In Australia, many financial and service industries have databases which collect the personal information of people who have a bad credit or real estate history, to name only two examples. Sometimes, one mistake years ago can follow you around longer than a HECS-HELP debt.

It's important to understand how your personal information will be used and if it can end up on a 'blacklist'. If something isn't clear – ASK!

If you're not happy with the answers and believe that the organisation isn't doing the right thing under the Privacy Act, see www.privacy.gov.au or call 1300 363 992 for advice about the Office of the Privacy Commissioner's complaints process.

The reality is that your name could end up on a 'blacklist'

Top ten hints for keeping your personal information private

- 1. Ask why your information is needed** – what are they going to use it for?
- 2. Think before you disclose** – you may not need to hand out your personal information
- 3. Don't put large amounts of personal information on social networking sites**
- 4. Check your records** – make sure your information is correct and up to date
- 5. Read privacy policies** – can be boring, but informative!
- 6. Don't leave your personal information lying around** – shred old mail and records
- 7. Sign up to the 'Do Not Call Register'** – visit www.donotcall.gov.au
- 8. Check security procedures when using Internet cafes**
- 9. Tick the 'opt out' box on forms**
- 10. Know your privacy rights** – visit www.privacy.gov.au

Copyright © 2009. *Private i* is an informal publication and should not be relied upon for legal advice. You may need to consult a lawyer for advice on specific matters.



Australian Government
Office of the Privacy Commissioner

Office of the Privacy Commissioner
1300 363 992
TTY 1800 620 241 no voice calls
GPO Box 5218
Sydney NSW 2001
www.privacy.gov.au