



Australian
Competition &
Consumer
Commission

THE LITTLE BLACK BOOK OF **SCAMS**



Australian
Competition &
Consumer
Commission

THE LITTLE BLACK BOOK OF **SCAMS**

Your guide to scams, swindles, rorts and rip-offs

Australian Competition and Consumer Commission
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

First published by the ACCC 2008

This revised edition published by the ACCC 2011

Illustrations by Pat Campbell

© Commonwealth of Australia 2011

This work is copyright. Apart from any use permitted under the *Copyright Act 1968*, no part may be reproduced without prior written permission from the Australian Competition and Consumer Commission. Requests and inquiries concerning reproduction and rights should be addressed to the Director Publishing, ACCC, GPO Box 3131, Canberra ACT 2601, or publishing.unit@accc.gov.au.

Important notice

The information in this publication is for general guidance only. It does not constitute legal or other professional advice, and should not be relied on as a statement of the law in any jurisdiction. Because it is intended only as a general guide, it may contain generalisations. You should obtain professional advice if you have any specific concern.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

ISBN 978 1 921393 22 8

ACCC 09/11_23268_425

www.scamwatch.gov.au

CONTENTS

Introduction	5
Lotteries, sweepstakes and competitions	6
Chain letters and pyramid scams	8
Golden investment opportunities	10
Betting and computer prediction software	12
Money transfer requests	14
Banking, credit card and online account scams	16
Internet scams	18
Mobile phone scams	20
Health and medical scams	22
Psychic and clairvoyant scams	24
Dating and romance scams	26
Charity scams	28
Door-to-door scams	30
Job and employment scams	32
Small business scams	34
Scams DO happen	36
Handy hints to protect yourself	38
Scams and you: what to do if you get scammed!	40
Getting help and reporting a scam	42



Myth busters

Busting these common myths will minimise your chances of being scammed.

- All companies, businesses and organisations are legitimate because they are approved and monitored by the government. **This is not always true.** While there are rules about setting up and running a business or a company in Australia, scammers can easily pretend to have approval when they don't. Even businesses that do have approval to operate could still try and scam you by acting dishonestly.
- All internet websites are legitimate. **This is not always true.** Websites are quite easy and cheap to set up and there are not many checks in place to ensure that a website is legitimate.
- There are short cuts to wealth that only a few people know. **This is not always true.** Ask yourself the question: if someone knew a secret to instant wealth, why would they be telling their secret to others?
- Scams involve large amounts of money. **This is not always true.** Sometimes scammers target a large number of people and try to get a small amount of money from each person.
- Scams are always about money. **This is not always true.** Some scams are aimed at stealing personal information from you.

Golden rules

Remember these golden rules to help you beat the scammers.

- ✓ Always get independent advice if an offer involves money, time or commitment.
- ✓ There are no guaranteed get-rich-quick schemes—the only people who make money are the scammers.
- ✓ Do not agree to offers or deals straightaway. If you think you have spotted a great opportunity, insist on time to get independent advice before making a decision.
- ✓ Do not hand over money or sign anything until you have done your homework and checked the credentials of the company that you are dealing with.
- ✓ Do not rely on glowing testimonials: find solid evidence of a company's success.
- ✓ Log directly on to a website that you are interested in rather than clicking on links provided in an email.
- ✓ Never send money or give credit card or online account details to anyone you do not know and trust.
- ✓ If you spot a scam or have been scammed, get help. Contact the office of fair trading in your state or territory, the Australian Competition and Consumer Commission (ACCC) or the Australian Securities and Investments Commission (ASIC) for assistance.

Scammers are imaginative and manipulative. They know how to push your buttons to produce the response they want.

Introduction



Every year, Australians lose millions of dollars to the activities of scammers who bombard us with online, mail, door-to-door and telephone scams.

We are pleased to bring you a new edition of *The little black book of scams*. We hope this book will increase your awareness of the vast array of scams that target Australians and teach you some easy steps you can take to protect yourself.

Scams do not discriminate

Scams target people of all backgrounds, ages and income levels. Fake lotteries, advance-fee frauds, get-rich-quick schemes and miracle health cures are some of the favoured means of separating the unwary from their money. New varieties of these scams appear all the time.

The ACCC has seen the devastating effects scams can have on people and their families. One of the best ways to combat this kind of fraud is to help you take measures to prevent yourself being caught out in the first place.

Protect yourself

If you want to stay on top of scams, visit our SCAMwatch website (www.scamwatch.gov.au). SCAMwatch contains information on dozens of different scams targeting consumers and small businesses, tips on guarding against scams, victim stories from Australian consumers, regular scam alerts and advice on reporting a scam.

Just remember: if it sounds too good to be true, it probably is!

Lotteries, sweepstakes and competitions



Many Australians are lured by the excitement of a surprise win and find themselves sending huge amounts of money overseas to claim fake prizes.

What to look for

You cannot win money or a prize in a **lottery** unless you have entered it yourself, or someone else has entered it on your behalf. You cannot be chosen as a random winner if you don't have an entry.

Many lottery scams try to trick you into providing your banking and personal details to claim your prize. You should not have to pay any fee to claim a legitimate prize.

Don't be fooled by claims that the offer is legal or has government approval—all scammers will tell you this. Instead of receiving a grand prize or fortune, you will lose every cent that you send to a scammer. And if you have provided other personal details, your identity could be misused too.

Remember that tickets in legitimate Spanish lotteries or the UK Lotto can only be bought in that country.

A **fake prize** scam will tell you that you have won a prize or a competition. You may receive an email, a text message or see a pop-up screen on your computer. There are often costs involved with claiming your prize, and even if you do receive a prize it may not be what was promised to you.

The scammers make their money by making you pay fees or call their premium rate phone numbers (usually starting with 19) to claim your prize. These premium rate calls can be very expensive, and the scammers will try to keep you on the line for a long time or ask you to call a different premium rate number.



PROTECT YOURSELF

REMEMBER

Legitimate lotteries do not require you to pay a fee to collect winnings.

CAUTION

Never send money to anybody you don't know and trust.

THINK

Don't provide personal banking details to anyone that you do not know or trust.

INVESTIGATE

Examine all of the terms and conditions of any offer very carefully—claims of free or very cheap offers often have hidden costs. Calls or text messages to premium rate phone numbers (starting with 19) can be very expensive.

ASK YOURSELF

Did I enter this competition? You cannot win money or a prize in a competition unless you have entered it yourself, or someone else has entered it on your behalf.

Chain letters and pyramid scams



Chain letters and pyramid schemes promise a large financial return for a relatively small cost. Pyramid schemes are illegal and very risky—and can cost you a lot of money.

What to look for

In a typical **pyramid scheme**, unsuspecting investors are encouraged to pay large up-front joining or membership fees to participate in money-making ventures. The only way for you to ever recover any money is to convince other people to join and to part with their money as well. People are often persuaded to join by family members or friends. But there is no guarantee that you will recoup your initial investment.

Although pyramid schemes are often cleverly disguised, they make money by recruiting people rather than by selling a legitimate product or providing a service. Pyramid schemes inevitably collapse and you will lose your money.

In Australia, it is a crime to promote a pyramid scheme or even to participate in one.

Be cautious, but do not be discouraged from carefully researching other business opportunities

based on commissions. There are many legitimate multi-level marketing opportunities where you can legally earn an income from selling genuine products or services.

Chain letters operate in a similar manner—you will be asked to send a small amount of money or a particular gift to everyone listed in the letter. You then put your name on the bottom of the list and send out copies of the letter to as many people as you can. The letter claims that by doing this, you will receive a large amount of money or a gift in a short space of time.

In a chain letter scam you lose your money in two ways: first, you send money to the scammers who sent you the letter; second, you waste a lot of money on postage and photocopying.



PROTECT YOURSELF	REMEMBER	Chain letters and pyramid schemes may be sent to you from family members and people you trust—they might not know that they could be illegal or that they are involved in a scam.
	CAUTION	Never commit to anything at high-pressure meetings or seminars.
	THINK	Don't make any decisions without doing your homework—research the offer being made and seek independent advice before making a decision.
	INVESTIGATE	Do some research on all business opportunities that interest you.
	ASK YOURSELF	If I am not selling a genuine product or service, is participation in this activity legal?

Golden investment opportunities



Have you been tempted to invest in high-risk money-making schemes promising ‘risk-free investment’? Often the return is nothing but misfortune.

What to look for

If you are trying to fast-track your way to wealth, don’t rely on the information you hear at an **investment seminar**. While investment advice can be legitimate and helpful, many scammers use the hype and buzz of a seminar to promote their property and investment scams.

The investments on offer are often over-valued and investors are later hit with fees and commissions that the promoters did not disclose. Incentives such as ‘limited opportunity’ or ‘rent guarantees’ may not deliver the benefits they promise when the total cost of the deal is taken into account.

Even if you don’t invest, the scammer can make a lot of money by charging attendance fees for seminars and courses, and by selling reports or books that may not be worth their asking price.

Cold calling is an unexpected or unsolicited telephone call from someone you don’t know offering you an investment opportunity or financial advice.

The opportunities offered by cold calling are usually share, mortgage or real estate ‘investments’, ‘high-return’ schemes, option trading or foreign currency trading. The scammers tend to operate from overseas as most of their activities are illegal in Australia.

Cold calling about financial products or services is illegal if the caller does not have an Australian Financial Services licence. A scammer could give you fake details, so you really need to do your homework.

Share promotion and **hot tip** scams usually come to you by a spam email or a phone message encouraging you to invest in a company whose shares are predicted to increase in value. Based on this anonymous tip, the scammer hopes that new investors will buy the stock and send the price soaring. The scammer will then sell off their shares at the new high price and make a profit. This selling generally drives the share price down dramatically, and people who bought the shares can be left with large losses.



PROTECT YOURSELF

REMEMBER	Be wary of investments promising a high return with little or no risk and avoid the 'get rich quick' pushers. Generally, the higher the promised return, the higher the risk of loss involved.
CAUTION	Never rush—take your time and seek independent advice before making any investment decision.
THINK	Don't commit to any investment at a seminar—the atmosphere at these events can be quite charged and exciting.
INVESTIGATE	If someone tries to offer you an investment or other financial service, ask for their Australian Financial Services licence number and take the time to confirm their details by calling ASIC.
ASK YOURSELF	If a stranger knew for certain a quick way to make money, would they really be telling you?

Betting and computer prediction software



Australians love gambling. Don't be tempted to buy software packages that claim they can predict results with a high degree of accuracy. Gambling is risky and there is no guarantee that you will make a profit.

What to look for

Gambling software packages promise to accurately predict the results of horse races, sports events or movements in the share market. Huge returns are promised based on past results and trends. But when they fail to work, refunds are hard to come by. Scammers can charge a lot of money for these systems, ranging from around \$1000 to more than \$15 000.

There are legitimate software programs to help people monitor share prices, but the scammers go one further and claim that their software can accurately predict movements in share prices. Past performance is not a guarantee of future performance when evaluating the results advertised.

Betting software scams claim that the predictions are based on weather conditions, the condition of the horse, the draw or the condition of the jockey. It promises huge returns based on past results and trends. However, once you buy it and it does not work as promised, you won't get your money back. Scammers usually advertise these systems as business opportunities or investments (or approach you through unsolicited emails, letters or phone calls). They often target professional people or those getting close to retirement.



PROTECT YOURSELF

REMEMBER

Even if a promoter tells you that a scheme or program has the endorsement of a respectable betting agency or share trading company, you should always seek advice from an independent professional.

CAUTION

Never think you won't be targeted because you are not a gambler. Sometimes these schemes are promoted as an 'investment program', not a gambling or punting system.

THINK

Don't be fooled by claims of high accuracy or high strike rates. It's easy for a scammer to manipulate the statistics and give you the impression that a system will be highly profitable for you.

INVESTIGATE

If you are interested in a software package that you think may assist you to manage or monitor your investments, seek advice from an independent professional before making any decisions.

ASK YOURSELF

If someone can accurately predict gambling results, why would they need to sell their secret to earn money?

Money transfer requests



Money transfer scams are on the rise. Be very careful when someone offers you money to help transfer their funds. Once you send money to someone, it can be very difficult, if not almost impossible, to get it back.

What to look for

The **Nigerian scam** is one of the most complained about scams in Australia. Although many of these sorts of scams originate in Nigeria, similar scams have been started by scammers all over the world (particularly in other parts of West Africa and in Asia). These scams are increasingly referred to as '**advance fee fraud**'.

In the classic Nigerian scam, you receive an email or letter from a scammer asking your help to transfer a large amount of money overseas. You are then offered a share of the money if you agree to give them your bank account details to help with the transfer. They will then ask you to pay all kinds of taxes and fees before you can receive your 'reward'. You will never be sent any of the money, and will lose the fees you paid.

Then there is the scam email that claims to be from a lawyer or bank representative advising that a long-lost relative of yours has died and left you a huge **inheritance**. Scammers can tell such genuine sounding stories that you could be tricked into providing personal documents and bank account details so that you can

confirm their identity and claim your inheritance. The 'inheritance' is likely to be non-existent and, as well as losing any money you might have paid to the scammer in fees and taxes, you could also risk having your identity stolen.

If you or your business is selling products or services online or through newspaper classifieds, you may be targeted by an **overpayment** scam. In response to your advertisement, you might receive a generous offer from a potential buyer and accept it. You receive payment by cheque or money order, but the amount you receive is more than the agreed price. The buyer may tell you that the overpayment was simply a mistake or they may invent an excuse, such as extra money to cover delivery charges. If you are asked to refund the excess amount by money transfer, be suspicious. The scammer is hoping that you will transfer the refund before you discover that their cheque has bounced or their money order was phony. You will lose the transferred money as well as the item if you have already sent it.



PROTECT YOURSELF



REMEMBER

If you have been approached by someone asking you to transfer money for them, make sure that it is from a legitimate source.

CAUTION

Never send money, or give credit card or online account details to anyone you do not know and trust.

THINK

Don't accept a cheque or money order for payment for goods that is more than what you agreed upon. Send it back and ask the buyer to send you payment for the agreed amount before you deliver the goods or services.

INVESTIGATE

Examine the information on SCAMwatch (www.scamwatch.gov.au) for information on how to protect yourself against money transfer scams.

ASK YOURSELF

Is it really safe to transfer money for someone you do not know?

Banking, credit card and online account scams



Advances in technology have changed the way we do our banking and pay for goods and services. Scammers use new technology to their advantage to come up with new scams to steal your bank account information and your money. Watch out for the warning signs.

16

What to look for

Phishing scams are all about tricking you into handing over your personal and banking details to scammers. The emails you receive might look and sound legitimate but in reality genuine organisations like a bank or a government authority will never expect you to send your personal information by an email or online.

Scammers can easily copy the logo or even the entire website of a genuine organisation. So don't just assume an email you receive is legitimate. If the email is asking you to visit a website to 'update', 'validate' or 'confirm' your account information, be sceptical.

Delete phishing emails. They can carry viruses that can infect your computer. Do not open any attachments or follow any links in phishing emails.

A **fake fraud alert** is similar to a phishing scam. The scammer will contact you by email or phone and tell you there is a problem with your account. To fix the problem or upgrade the security of your account, they will ask you to confirm all your personal details. Scammers have been known to make up all sorts of stories to trick their victims.

Some people are told that their credit card has been used to make a suspicious purchase in a foreign country and others have simply been told that their details are needed for a security and maintenance upgrade.

Banks and financial institutions will often contact people to alert them to suspicious activity on their account, but they will never ask you to provide your details online or over the phone. If in doubt, ring the bank yourself.

Card skimming is the copying of information from the magnetic strip of a credit card or ATM card. Once scammers have skimmed your card, they can create a fake or 'cloned' card with your details to make charges on your account. Or they may simply photocopy your card and use the details.

Be suspicious if a shop assistant insists on taking your card out of your sight to process your transaction or tries to swipe your card through more than one machine. If the machine doesn't look right to you, don't use it.



PROTECT YOURSELF	REMEMBER	A legitimate bank or financial institution will never ask you to click on a link in an email or send your account details through an email or website.
	CAUTION	Never send your personal, credit card or account information by an email or enter it on a website that you are not certain is genuine.
	THINK	Don't give out your personal, credit card or account details over the phone unless you made the call and the phone number came from a trusted source.
	INVESTIGATE	SCAMwatch (www.scamwatch.gov.au) has links to websites with the latest information and tips on how to protect yourself online. Keep your security software up to date to detect and remove viruses and other malicious software. A computer professional can advise you about this.
	ASK YOURSELF	Are the contact details provided in an email correct? Telephone your bank or financial institution to ask whether the email you received from them is genuine. Use a phone number that you know is legitimate, from an account statement, the phone book or the back of your ATM card — do not rely on the contact details provided in the email.

Internet scams



A lot of internet scams take place without the victim even noticing. You can greatly reduce the chances of being scammed on the internet if you follow some simple precautions.

What to look for

Scammers can use the internet to promote fraud through unsolicited or junk emails, known as **spam**. Even if they only get a handful of replies from the millions of emails they send out, it is still worth their while. Be wary of replying, even just to 'unsubscribe', because that will give a scammer confirmation that they have reached a real email address.

Any email you receive that comes from a sender you do not know, is not specifically addressed to you and promises you some benefit is likely to be spam.

Malicious software—also referred to as malware, spyware, key loggers, trojan horses, or trojans—poses online security threats. Scammers try to install this software on your computer so that they can gain access to files stored on your computer and other personal details and passwords.

Scammers use a wide range of tricks to get their software onto your computer. They may trick you into clicking on a link or pop-up message in a spam email or by getting you to visit a fake website set up solely to infect people's computers.

Online auctions and **internet shopping** can be a lot of fun and can also help you find good deals. Unfortunately, they also attract scammers.

Scammers will often try to get you to deal outside of online auction sites. They may claim the winner of an auction that you were bidding on has pulled out and offer the item to you. Once you have paid, you will never hear from them again and the auction site will not be able to help you.

Malware is programming or files developed for the purpose of doing harm. Malware includes computer viruses, worms and trojan horses.

Spyware is software installed on a computing device that takes information from it without the consent or knowledge of the user and gives that information to a third party. Spyware is an intelligence-gathering tool—it is used to literally spy on people and collect information about them. People who install spyware may be targeting information such as banking and credit card details or other sensitive commercial or private information. They may take this information for their own use or give it to another person.

A **trojan horse** contains malicious or harmful coding in apparently harmless programming or data that can take control and do its chosen form of damage, such as ruining the hard disk. A trojan horse may be widely redistributed as part of a computer virus and you may not be aware that it is on your computer.

A **key logger** is software that logs a user's keystrokes as they type to capture private information, passwords or credit card or financial information. Occasionally, key loggers can be physical devices attached to a computer.



PROTECT YOURSELF

REMEMBER

If you choose to shop online or participate in online auctions, make sure you know about refund policies and dispute-handling processes and be careful that you are not overcharged. Also, you may want to use an escrow service. This service will hold your payment and only release it to the seller once you have confirmed that you received what you paid for. There is usually a small fee for this service.

CAUTION

Never buy from bidders with poor ratings on auction sites, and do your best to ensure that you are only making purchases from genuine shopping sites.

THINK

Don't reply to spam emails, even to unsubscribe, and do not click on any links or call any telephone number listed in a spam email. Make sure you have current protective software or get advice from a computer specialist.

INVESTIGATE

If an email or pop-up offers you a product or service that genuinely interests you and it seems reasonable, be sure that you understand all the terms and conditions and costs involved before making a purchase or providing your details.

ASK YOURSELF

By opening this suspect email, will I risk the security of my computer?

Mobile phone scams



Mobile phone scams can be difficult to recognise. Be wary of somebody who talks as if they know you or of redialling a missed call from an unknown number—there may be hidden charges.

What to look for

Ringtone scams might attract you with an offer of a free or low-cost ringtone. What you may not realise is that by accepting the offer, you are actually subscribing to a service that will keep sending you ringtones—and charging you a premium rate for them. There are many legitimate companies selling ringtones, but there are also scammers who will try to hide the true cost of taking up the offer.

Scammers either don't tell you that your request for the first ringtone is actually a subscription to a ringtone service, or it may be obscured in fine print related to the offer. They also make it difficult for you to stop the service. You have to actively 'opt out' of the service to stop the ringtones and the associated charges.

Missed call scams start by scammers ringing your phone and hanging up so quickly that you can't answer the call in time. Your phone registers a missed call and you probably won't recognise the number. You may be tempted to call the number to find out who called you. If it is a scam, you will be paying premium rates for the call without knowing.

Text message scams work in a similar way, but through SMS. Scammers send you a text message from a number you may not recognise, but it sounds like it is from a friend—for instance, 'Hi, it's John. I'm back! When are you free to catch up?' If you reply out of curiosity, you might be charged at premium rate for SMS messages (sometimes as much as \$4 for each message sent and/or received).

An **SMS competition** or **SMS trivia** scam usually arrives as a text message and may encourage you to enter a competition for a great prize. The message (or sometimes, an advertisement) could also invite you to take part in a trivia competition with a great prize on offer if you answer a certain number of questions correctly. The scammers make money by charging extremely high rates for the messages you send and any further messages they send to you. With trivia scams, the first lot of questions will be very easy. This is meant to encourage you to keep playing. However, the last one or two questions that you need to answer to claim your 'prize' could be very difficult or impossible to answer correctly.



PROTECT YOURSELF



REMEMBER

Text 'STOP' to unwanted text messages or to end unwanted subscriptions.

CAUTION

Never reply to text messages offering you free ringtones or missed calls from numbers that you do not recognise.

THINK

Don't ring or text phone numbers beginning with 19 unless you are aware of the cost involved.

INVESTIGATE

Read all the terms and conditions of an offer very carefully. Services offering free or very cheap products often have hidden costs.

ASK YOURSELF

Do you know how to stop any subscription service you want to sign up to?

Health and medical scams



Medical scams prey on human suffering. They offer solutions where none exist or promise to simplify complex health treatments.

What to look for

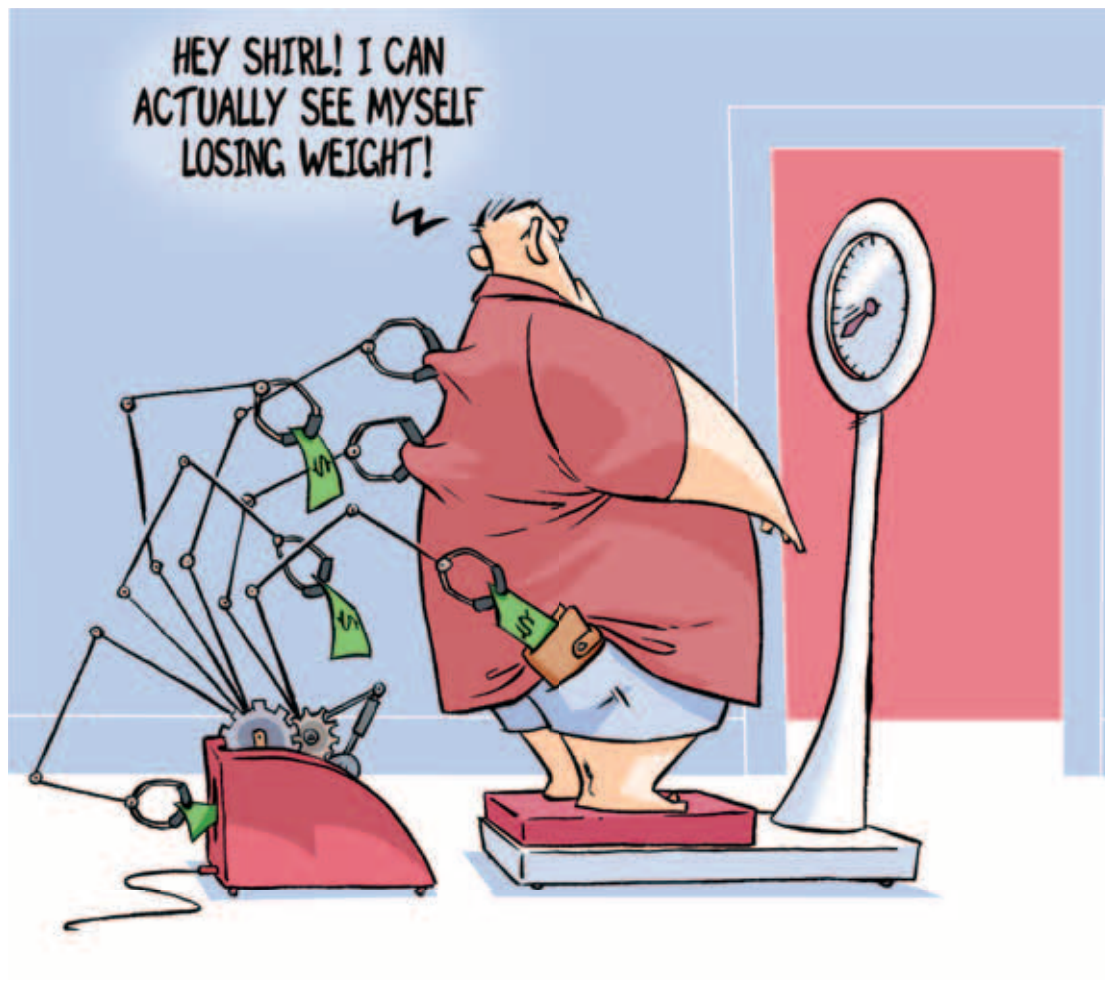
Miracle cure scams offer a range of products and services that can appear to be legitimate alternative medicines, usually promising quick and effective remedies for serious medical conditions. The treatments claim to be effective against a very wide range of ailments and are often promoted using testimonials from people who have used the product or service and have been 'cured'.

Weight loss scams promise dramatic weight loss with little or no effort. This type of scam may involve an unusual or restrictive diet, revolutionary exercise or 'fat-busting' devices, or breakthrough products such as pills, patches or creams. The products are promoted with the use of false claims such as 'lose 10 kilos in 10 days' or 'lose weight while you sleep' and often require large

advance payments or that you enter into a long-term contract to participate in the program.

Fake online pharmacies use the internet and spam emails to offer drugs and medicine at very cheap prices and/or without the need for a prescription from a doctor. If you use such a service and you actually do receive the products that you order, there is no guarantee that they are the real thing.

There are legitimate online pharmacies. These businesses will have their full contact details listed on their website and will also require a valid prescription before they send out any medicine that requires one.



PROTECT YOURSELF

REMEMBER

There are no magic pills, miracle cures or safe options for rapid weight loss.

CAUTION

Never commit to anything under pressure.

THINK

Don't trust an unsubstantiated claim about medicines, supplements or other treatments. Consult your healthcare professional.

INVESTIGATE

Ask for published medical and research papers to support the claims made by the promoters.

ASK YOURSELF

If this really is a miracle cure, wouldn't your healthcare professional have told you about it?

Psychic and clairvoyant scams



Psychic or clairvoyant scams have been around for a long time. Scammers often offer you their secrets to wealth and other plans or insights that they claim will bring you good fortune and money.

What to look for

A **psychic** or **clairvoyant** scam can come to you in many ways: through the post, in an email, by a telephone call or even face-to-face.

Generally, a psychic or clairvoyant scammer will claim to know that you are in some sort of trouble and offer you a solution—for a fee. This ‘solution’ could be some winning lottery numbers, a lucky charm or the removal of a curse or jinx.

Scammers may also try and talk you into buying their ‘secret of wealth’ or other plans or ‘insights’ that they claim will change the course of your life forever.

Scammers make money by charging you to claim your lucky charm or secret to wealth and sending you a worthless item—or nothing at all—in return.

Psychic scams can also be used to set you up to fall for a lottery scam too. If a psychic gives you a list of lucky lottery numbers, don’t be surprised if you receive a letter soon afterwards telling you that you’ve just won a lottery you’ve never heard of and do not remember entering. Don’t get stung twice—refer to page 6 to read about lottery scams.

The psychic or clairvoyant may try to convince you that they are genuine by telling you something about yourself. Is what they are telling you vague or general? It could therefore be true of anyone.



PROTECT YOURSELF

REMEMBER

Psychic and clairvoyant scams prey on your curiosity.

CAUTION

Never send money or give credit card or online account details to anyone you do not know and trust. If the offer came in an email, do not respond to the email and do not try to unsubscribe. This will only confirm to the scammers that your email address is active.

THINK

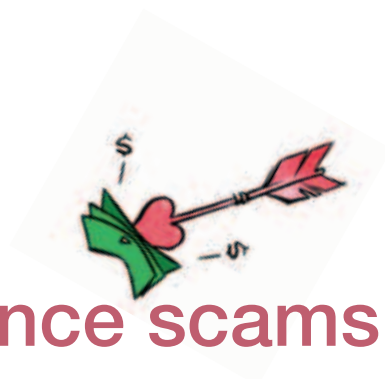
Take a step back and carefully consider any advice or suggestions given by someone who claims to be a psychic.

INVESTIGATE

Examine whether there is any evidence to support the claims made by the psychic or clairvoyant.

ASK YOURSELF

Am I putting myself and my family or friends at risk by acting on the random advice of a stranger?



Dating and romance scams

Despite the many legitimate dating websites operating in Australia, there are many dating and romance scams as well. Dating and romance scams try to lower your defences by appealing to your romantic and compassionate side.

What to look for

Some **dating and romance** scams work by setting up a dating website where you pay for each email or message you send and receive. The scammer will try to hook you in by continuing to send you vague-sounding emails filled with talk of love or desire. The scammer might also send emails filled with details of their home country or town that do not refer to you much at all. These are attempts to keep you writing back and paying money for use of the scammer's dating website.

Even on a legitimate dating site, you might be approached by a scammer—perhaps someone who claims to have a very sick family member or who is in the depths of despair (often these scammers claim to be from Russia or Eastern Europe). After they have sent you a few

messages, and maybe even a glamorous photo, you will be asked (directly or more subtly) to send them money to help their situation. Some scammers even arrange to meet with you, in the hope that you give them presents or money—and then they disappear.

In other cases, scammers will try to build a friendship with you, perhaps even sending you flowers or other small gifts. After building a relationship, the scammer will tell you about a large amount of money they need to transfer out of their country, or that they want to share with you. They will then ask for your banking details or money for an administrative fee or tax that they claim needs to be paid to free up the money.



PROTECT YOURSELF

REMEMBER

Check website addresses carefully. Scammers often set up fake websites with very similar addresses to legitimate dating websites.

CAUTION

Never send money or give credit card or online account details to anyone you do not know and trust.

THINK

Don't give out any personal information in an email or when you are chatting online.

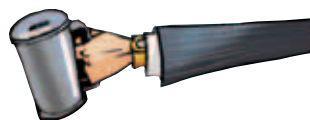
INVESTIGATE

Make sure you only use legitimate and reputable dating websites.

ASK YOURSELF

Would someone you have never met really declare their love for you after only a few letters or emails?

Charity scams



Charity scams take advantage of people's generosity and kindness by asking for donations to a fake charity or by impersonating a real charity.

What to look for

Charity scams involve scammers collecting money by pretending to be a real charity. The scammers can approach you in many different ways—on the street, at your home, over the phone or on the internet. Emails and collection tins may even be badged with the logos of genuine charities.

Often, the scammer will exploit a recent natural disaster or famine that has been in the news. Other scammers play on your emotions by pretending to be from charities that help children who are ill.

Scammers can try to pressure you to give a donation and may give false, or refuse to give, details about the charity, such as their address or their contact details.

Not only do these scams cost people money; they also divert much needed donations away from legitimate charities and causes. Luckily these types of scams are not that common.

Legitimate charities are registered at the state or territory level. Call your local fair trading agency to check that the charity that has approached you is genuine. If the charity is genuine and you want to make a donation, get the charity's contact details from the phone book or a trusted website.

If you do not want to donate any money, or you are happy with how much you may have donated to charities already, simply ignore the email or letter, hang up the phone or say no to the person at your door. You do not have to give any money at all.



PROTECT YOURSELF



REMEMBER

If you have any doubts at all about the person asking for money, do not give them any cash, credit card or bank account details.

CAUTION

Never give out your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.

THINK

If in doubt, approach an aid organisation directly to make a donation or offer support.

INVESTIGATE

Call your local fair trading agency to check that the charity that has approached you is genuine.

ASK YOURSELF

How and to whom would I like to make a contribution?

Door-to-door scams



Door-to-door sales can promote home maintenance services such as pest control, home and garden maintenance and even utilities such as electricity and telephone services. Many legitimate businesses sell things by going door-to-door, but some scammers also use this approach.

What to look for

Door-to-door scams involve promoting goods or services that are not delivered or are of a very poor quality. You will not get value for money from a scammer and you may get billed for work that you didn't want or didn't agree to.

Sometimes scammers pretend to conduct a survey so they can get your personal details or to disguise their sales pitch until they have been talking to you for a while. At worst, a doorknocker's real purpose could be to prepare for a subsequent break-in into your home.

Door-to-door sales are normally uninvited. Sometimes the salesperson just turns up at your door. Salespeople are not visitors in your home—

they are there to get you to hand over your money to them and they must leave if you ask them to.

Even in the case of genuine businesses and products, unscrupulous operators can still act illegally to the detriment of other people. Laws about door-to-door sales exist nationally and across all Australian states and territories, including laws relating to cooling-off periods—where you may be able to change your mind and request your money back.

If you are interested in what a door-to-door salesperson has to offer, take the time to find out about their business and their offer. Don't forget to shop around to make sure you are getting a good deal.



PROTECT YOURSELF



REMEMBER

If someone comes to your door, ask to see their identification. You do not have to let them in and they must leave if you ask them to.

CAUTION

Never agree to anything without reading all the terms and conditions of every offer very carefully—claims of free or very cheap offers often have hidden costs.

THINK

Don't agree to any offer involving a significant amount of money, time or commitment. Seek independent advice first.

INVESTIGATE

If you are interested in what a door-to-door salesperson has to offer, take the time to find out about their business and their offer. Shop around to make sure you are getting a good deal.

ASK YOURSELF

Is there a cooling-off period so that you can cancel a contract or purchase within a certain number of days? Contact the ACCC or your local fair trading agency for more information (see page 42 for contacts).



Job and employment scams

Job and employment scams target people looking for a new job or a change of job. They often promise a lot of income—sometimes they even guarantee it—for little or no effort.

What to look for

Work-from-home scams are often promoted through spam emails or advertisements on noticeboards. Most of these advertisements are not real job offers. Many of them are fronts for illegal money-laundering activity or pyramid schemes.

You might get an email offering a job where you use your bank account to receive and pass on payments for a foreign company. These 'job offers' promise that you will receive a percentage commission for each payment you pass on. Sometimes, scammers are just after your bank account details so they can access your account.

A **guaranteed employment** or **income** scam claims to guarantee you either a job or a certain level of income. The scammers usually contact you by spam email and the offers often involve the payment of an up-front fee for a 'business plan', certain start-up materials or software.

There are a range of scams promoted as **business opportunities**. You may be required to make an upfront payment (for something that does not work or is not what you expected) or to recruit other people to the scheme (refer to pyramid schemes on page 8).



PROTECT YOURSELF	REMEMBER	There are no shortcuts to wealth—the only people that make money are the scammers.
	CAUTION	Never send your bank account or credit card details to anybody you do not know and trust.
	THINK	Don't make any decisions without carefully researching the offer. Seek independent advice before making a decision.
	INVESTIGATE	Beware of products or schemes claiming to guarantee income and job offers requiring payment of an upfront fee. Make sure any franchise business opportunity is legitimate.
	ASK YOURSELF	Did I get all the details in writing before paying or signing anything?

Small business scams



Scams that target small business can come in a variety of forms—from bills for advertising or directory listings that were never ordered to dubious office supply offers.

What to look for

Small business operators and individuals with their own internet sites continue to be confused and caught out by unsolicited letters warning them that their internet domain name is due to expire and must be renewed, or offering them a new domain name similar to their current one.

If you have registered a domain name, be sure to carefully check any domain name renewal notices or invoices that you receive. While the notice could be genuine, it could also be from another company trying to sign you up, or it could be from a scammer.

- ✓ Check that the renewal notice matches your current domain name exactly. Look out for small differences—e.g. '.com.au' instead of '.net.au'.
- ✓ Check that the renewal notice comes from the company with which you originally registered your domain name.
- ✓ Check your records for the actual expiry date for your existing domain name.

A **directory entry or unauthorised advertising** scam tries to bill a business for a listing or advertisement in a magazine, journal or business register/directory.

The scam might come as a proposal for a subscription disguised as an invoice for an entry in a fake international fax, telex or trade directory.

You might also be led to believe that you are responding to an offer for a free entry when in fact the order is for entries requiring later payment.

Another common approach used by scammers is to call a firm asking to confirm details of an advertisement that they claim has already been booked. The scammer might quote a genuine entry or advertisement your business has had in a different publication or directory to convince you that you really did use the scammer's product.

A **faxback** scam can offer you anything from amazing diets to fantastic deals, business directory entries and competition entries—all you have to do is send a fax back to a premium rate number (starting with 19). Premium rate faxes can be charged at more than \$6.00 per minute. The scammers make sure your fax takes several minutes to get through, resulting in a high phone bill.

An **office supply** scam involves you receiving and being charged for goods that you did not order. These scams often involve goods or services that you regularly order—for example, paper, printing supplies, maintenance supplies or advertising.

You might receive a phone call from someone claiming to be your 'regular supplier', telling you that the offer is a 'special' or 'available for a limited time'. If you agree to buy any of the supplies offered to you, they will often be overpriced and bad quality.



PROTECT YOURSELF



REMEMBER

Make sure that the people processing the invoices or answering telephone calls are aware of these scams. They will most often be the point of contact for the scammers. Always check that goods or services were both ordered and delivered before paying an invoice.

CAUTION

Never give out or clarify any information about your business unless you know what the information will be used for.

THINK

Don't agree to a business proposal over the phone—always ask for an offer in writing. Limit the number of people in your business that have access to funds and have the authority to approve purchases.

INVESTIGATE

Effective management procedures can go a long way towards preventing these scams from succeeding. Having clearly defined procedures for the verification, payment and management of accounts and invoices is an effective defence against these types of scams.

ASK YOURSELF

If a caller claims that you have ordered or authorised something and you do not think it sounds right, shouldn't you ask for proof?

Scams DO happen

The lottery and sweepstakes scam

Robyn received an email with news that she had won US\$200 000 in the 'American Millennium Millions Sweepstakes'. The email said Robyn's email address was one of 10 addresses selected at random from a database of more than 500 000 people who had made an online purchase. Apparently the Millennium Millions Sweepstakes was part of a global promotion to encourage internet users to use the internet safely, and Robyn's online purchase had entered her in this lottery—she didn't need to buy a ticket.

As Robyn had recently purchased a coffee machine from an overseas auction site, she decided it was quite possible that she might have won a prize in this promotion. The email looked official and provided the government authorisation number for the competition. It also provided an email and phone number of a contact person at the 'Grand United Bank of South America', which administers the prize payment.

Robyn followed the links in the email to the website of the Millennium Millions and keyed in the secret PIN and reference number. The website flashed a message of congratulations and confirmed that Robyn was a winner. To claim her prize she had to register her details online and organise a money transfer of \$15 000 to cover taxes and insurance.

Robyn was very hesitant to send such a large amount of money, so she rang the 'Grand United Bank of South America' using the phone number listed in the email. The operator assured Robyn that her winnings would be released within seven days of the bank receiving her transfer. The gentleman was very encouraging and urged Robyn to act quickly to make her claim.

Robyn was very excited and went straight to her bank to organise the transfer. The bank teller thought the story sounded suspicious and urged Robyn to get professional advice before

proceeding. Eventually, Robyn decided to ring her son-in-law Darren and ask his opinion.

Darren told Robyn that fake lotteries and competitions were one of the most common scams around. He told her how easy it would be for the scammer to set up a fake website and send an email that looked authentic. He also pointed out to Robyn that the phone number that Robyn rang was part of the scam too. Darren convinced Robyn that the offer was a scam and that she mustn't send anything at all. Robyn was a bit deflated, but with hindsight agreed she was very lucky that she had not proceeded to give the scammers \$15 000 or any more of her personal details.

The inheritance (or Nigerian) scam

Brendan Macarthur received an email from Mr Henderson, a solicitor from a UK legal firm, advising him that he was the sole beneficiary of a deceased estate of Gavin Macarthur who had recently passed away in Scotland. Although Brendan advised Mr Henderson that he didn't know a Gavin Macarthur, he was assured by Mr Henderson that there was a distant relationship and that Brendan was legally entitled to claim the £150 000 inheritance.

When Mr Henderson provided Brendan with a death certificate for the deceased and an affidavit from 'High Court of London' confirming he was the next of kin, Brendan's hesitation turned to excitement. With a young family to support, £150 000 would set him up for life.

Brendan followed Mr Henderson's instructions to claim the money. Brendan provided copies of his passport and driver's licence to verify his identity and then supplied his bank account details so that the bank could transfer the funds directly into his account. Brendan even delayed a repayment on his mortgage so that he could pay the \$8000 in taxes and legal fees that Mr Henderson requested.

Brendan mentioned his good fortune to a few mates over a beer at the pub. One of his mates told Brendan that the whole thing sounded a lot like something he had seen recently on a television program where a whole bunch of scammers had been busted in West Africa. Brendan recognised many similarities and started to worry. He reported the conduct to the police and to the ACCC, and sought help from a community legal centre for advice. Unfortunately for Brendan, he was unable to recover the \$8000 he had paid to Mr Henderson, but by acting quickly and talking to his bank he was able to prevent any more money being drained from his account.

The advance fee fraud scam

Joe found an advertisement for a second-hand car on a car sales website. It sounded exactly what Joe was looking for and, as the price was well below what he had expected to pay, Joe contacted the seller immediately.

The seller confirmed the bargain price and explained that he had unexpectedly moved overseas and needed to sell the vehicle quickly to help finance his move. The seller confirmed all the details of the car and even removed the advertisement from the website so that Joe knew he was first in line. The seller advised Joe that an agent would contact him shortly to organise the payment and delivery of the vehicle.

Joe soon received an email from the agent instructing him on how to proceed with payment. Joe did not want the seller to re-advertise the car, so he acted quickly and organised the money transfer as requested. Joe got a confirmation of payment from the agent and a delivery date for the car, but that was it.

The car never turned up and Joe was never able to make contact with either the seller or the agent again. The scam cost Joe more than \$12 000 and, as Joe had sent the money overseas, there was little the Australian authorities could do to help.

The work from home scam

When Marissa's youngest child started school she decided it was time to return to work. Marissa searched the online classifieds and her local paper for a job that would fit in with her family duties, but suitable jobs were hard to find and she was getting discouraged.

When Marissa received an email advertising a 'choose your own hours and work from home' opportunity, Marissa was immediately interested. According to the advertisement, Marissa could earn \$1500 to \$3000 per month, plus bonuses. The position did not require specific experience; just a willingness to learn, access to a computer and the internet and good managerial skills. There were career opportunities too!

The position was in the area of transaction processing, which meant that Marissa would receive transfers from buyers, process them, and then send payment on to agents at the direction of the company. With her background in retail and her basic knowledge of computers and internet banking, Marissa was pretty sure the job would be perfect. Marissa responded to the email and provided some personal information as well as details of the bank account that she would be using to receive and transfer money from.

It was all too easy, and Marissa soon had herself all set up. For several hours each morning, Marissa would process transactions and organise transfers. Some were quite complicated and involved large amounts of money which made Marissa a bit nervous, but it was worth it as she was able to earn good bonuses for these transactions.

After several weeks, Marissa's bank notified her that her account had been frozen due to suspicious activity and asked her to come in to meet with the manager. The authorities became involved too, and Marissa was horrified to learn that she had been involved in an illegal money-laundering ring and she could have been prosecuted for her activities.

Marissa's dream work-from-home job turned into a nightmare for Marissa and her family, but eventually Marissa was able to assist authorities to trace some of the criminals involved.

Disclaimer: The names and stories are fictional and based on information received by the ACCC.

Handy hints to protect yourself

38

Protect your identity

- Only give out your personal details and information where it is absolutely necessary and when you trust the person you are speaking to or dealing with.
- Destroy personal information: don't just throw it out. You should cut up or shred old bills, statements or cards—for example, credit cards and ATM cards.
- Treat your personal details like you would treat money: don't leave them lying around for others to take.

Money matters

- Never send money to anyone that you don't know and trust.
- Do not send any money or pay any fee to claim a prize or lottery winnings.
- 'Jobs' asking you to simply use your own bank account to transfer money for somebody could be a front for money-laundering activity. Money laundering is a serious criminal offence.
- Avoid transferring or wiring any refunds or overpayments back to anyone you do not know.

The face-to-face approach

- If someone comes to your door, ask to see some identification. You do not have to let them in, and they must leave if you ask them to.
- Before you decide to pay any money, if you are interested in what a door-to-door salesperson has to offer, take the time to find out about their business and their offer.
- Contact the office of fair trading in your state or territory if you are unsure about a trader that comes to your door.

Telephone business

- If you receive a phone call from someone you do not know, always ask for the name of the person you are speaking to and who they represent. Verify this information by calling the company yourself.
- Do not give out your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.
- It is best not to respond to text messages or missed calls that come from numbers you do not recognise. Be especially wary of phone numbers beginning with 19. These may be charged at a higher rate than other numbers and can be very expensive.

Email offers

- Never reply to a spam email, even to unsubscribe—often, this just serves to ‘verify’ your address to scammers. The best course of action is to delete any suspicious emails without opening them.
- Turn off the ‘viewing pane’ as just viewing the email may send a verification notice to the sender that is a valid email address.
- Legitimate banks and financial institutions will never ask you for your account details in an email or ask you to click on a link in an email to access your account.
- Never call a telephone number or trust other contact details that you see in a spam email.

Internet business

- Install software that protects your computer from viruses and unwanted programs and make sure it is kept current. If you are unsure, seek the help of a computer professional.
- If you want to access a website, use a bookmarked link to the website or type the address of the website into the browser yourself. Never follow a link in an email.
- Check website addresses carefully. Scammers often set up fake websites with very similar addresses to legitimate websites.
- Beware of websites offering ‘free’ downloads (such as music, adult content, games and movies). Downloading these products may

install harmful programs onto your computer without you knowing.

- Avoid clicking on pop-up ads—this could lead to harmful programs being installed on your computer.
- Never enter your personal, credit card or online account information on a website that you are not sure is genuine.
- Never send your personal, credit card or online banking details through an email.
- Avoid using public computers (at libraries or internet cafes) to do your internet banking or online shopping.
- When using public computers, clear the history and cache of the computer when you finish your session.
- Be careful when using software on your computer that auto-completes online forms. This can give internet scammers easy access to your personal and credit card details.
- Choose passwords that would be difficult for anyone else to guess—for example, passwords that include letters and numbers. You should also regularly change passwords.
- When buying anything online, print out copies of all transactions and only pay via a secure site. If using an internet auction site, note the ID numbers involved and read all the security advice on the site first.

Scams and you: what to do if you get scammed!

Australian authorities may not always be able to take action against scams, even if it seems like a scammer might have broken the law.

REDUCING THE DAMAGE

Although it may be hard to recover any money that you have lost to a scam, there are steps you can take to **reduce the damage** and avoid becoming a target for a follow-up scam. The quicker you act, the more chance you have of reducing your losses.

Report a scam. By reporting the scam to authorities, they may be able to warn other people about the scam and minimise the chances of the scam spreading further. You should also warn your friends and family of any scams that you come across. Details on how to report a scam are on page 42 of this publication.

If you have been tricked into signing a contract or buying a product or service

Contact the fair trading agency in your state or territory and consider getting independent advice to consider your options: there may be a cooling-off period or you may be able to negotiate a refund (especially if the seller is located in Australia).

If you think someone has gained access to your online account, telephone banking account or credit card details

Call your financial institution immediately so they can suspend your account and limit the amount of money you lose. Credit card companies may also be able to perform a 'charge back' (reverse the transaction) if they believe that your credit card was billed fraudulently.

Do not use contact details that appear in emails or on websites that you are suspicious of—they will probably be fake and lead you to a scammer. You can find legitimate contact details in the phone book, an account statement or on the back of your ATM card.

If the scam relates to your health

Stop taking any pills or substances that you are not sure about. See a doctor or other qualified medical professional as soon as you can. Be sure to tell them about the treatment that the scammer sold (take along any substances, including their packaging). Also tell them if you have stopped any treatment that you were on before the scam.

If you have sent money to someone that you think may be a scammer

If you sent your credit card details, follow the instructions in the section above.

If you sent money through an electronic funds transfer (over the internet), contact your financial institution immediately. If they have not already processed the transfer, they may be able to cancel it.

If you sent a cheque, contact your financial institution immediately. If the scammer hasn't already cashed your cheque, they may be able to cancel it.

If you sent money through a wire service (such as Western Union), contact the wire service immediately. If you are very quick, they may be able to stop the transfer.

If you have been tricked by a door-to-door seller or trader

You may be protected by laws that provide you with a 'cooling-off' period, during which you can cancel an agreement or contract that you signed. Contact the fair trading agency in your state or territory for advice about door-to-door sales laws.

If you have been scammed using your computer

If you were using your computer when you got scammed, it is possible that a virus or other malicious software is still on your computer. Run a full system check using reliable security software.

If you do not have security software (such as virus scanners and a firewall) installed on your computer, a computer professional can help you choose what you need.

Scammers may have also gained access to your online passwords. Change these using a secure computer.

If the scam involves your mobile phone

Call your telephone company and let them know what has happened.

Getting help and reporting a scam

The best agency to contact depends on where you live and what type of scam is involved.

If you think you have spotted a scam or have been targeted by a scam, there are many government agencies in Australia that you can contact for advice or to make a report. This may help you and prevent others from being ripped off by scam operators.

SCAMS FROM INTERSTATE OR OVERSEAS: CONTACT THE ACCC

The ACCC is the only national agency dealing with general consumer protection matters.

The Infocentre is the primary contact point of the ACCC. If appropriate, information received is passed on to investigators.

Infocentre 1300 302 502
www.accc.gov.au

Financial and investment scams should be reported to ASIC (see below).

SCAMwatch

SCAMwatch is a website run by the ACCC that provides information about how to recognise, avoid and report scams. Scams reported to SCAMwatch will be analysed by the ACCC.
www.scamwatch.gov.au

LOCAL SCAMS—CONTACT YOUR LOCAL CONSUMER AFFAIRS AGENCY

Your local consumer affairs agency is best placed to investigate scams that appear to come from within your own state or territory.

Some of the agency websites given below list specific scams operating in their state or territory and provide information on how to avoid being scammed and how to protect yourself.

NEW SOUTH WALES

NSW Fair Trading
13 32 20
www.fairtrading.nsw.gov.au

QUEENSLAND

Office of Fair Trading
13 13 04
www.fairtrading.qld.gov.au

SOUTH AUSTRALIA

Office of Consumer and Business Affairs
(08) 8204 9777
www.ocba.sa.gov.au

AUSTRALIAN CAPITAL TERRITORY

Office of Regulatory Services
(02) 6207 0400
www.ors.act.gov.au

VICTORIA

Consumer Affairs Victoria
1300 55 81 81
www.consumer.vic.gov.au

WESTERN AUSTRALIA

Department of Commerce
1300 30 40 54
www.commerce.wa.gov.au

TASMANIA

Consumer Affairs and Fair Trading
1300 654 499
www.consumer.tas.gov.au

NORTHERN TERRITORY

Consumer Affairs
1800 019 319
www.consumeraffairs.nt.gov.au

FINANCIAL AND INVESTMENT SCAMS—CONTACT ASIC

Financial scams involve sales offers or promotions about financial products and services such as superannuation, managed funds, financial advice, insurance, credit or deposit accounts.

You can report financial scams to the Australian Securities and Investment Commission on its Infoline or by accessing its website.

Australian Securities and Investments
Commission 1300 300 630
www.asic.gov.au

REPORTING BANKING AND CREDIT CARD SCAMS—CONTACT YOUR BANK OR FINANCIAL INSTITUTION

As well as reporting these scams to ASIC or the ACCC, you should alert your bank or financial institution about any suspicious correspondence that you receive about your account. They can advise you on what to do next.

Make sure that the telephone number you use is from the phone book, your account statement or the back of your credit or ATM card.

REPORTING SPAM EMAILS AND SMS—CONTACT ACMA

Many scams arrive by email and SMS. You can report uninvited emails (known as spam emails) to the Australian Communications and Media Authority on its website, www.spam.acma.gov.au and you can forward uninvited SMS (known as spam SMS) to the ACMA through its Spam SMS service—0429 999 888.

Fraudulent (or ‘phishing’) emails requesting personal details can also be reported to the bank, financial institution or other organisation concerned (be sure to use a phone number or email address that did not appear in the email to make your report).

REPORTING FRAUD, THEFT AND OTHER CRIMES—CONTACT THE POLICE

Many scams that may breach consumer protection laws (those enforced by the ACCC, ASIC and fair trading agencies) may also breach the fraud provisions of various crime acts.

If you are the victim of fraud—if you have suffered a loss because of someone’s dishonesty or deception—you should consider contacting your local police station (especially if the amount involved is significant).

You should definitely contact the police if you have had your property stolen or have been threatened or assaulted by a scammer.



SCAMwatch

Don't let scams sneak under your radar!

Stay one step ahead of the scammers. Read The little black book of scams and then visit SCAMwatch online to get the low-down on scams that target Australian consumers and small businesses.

Find out more about how scams work and how to protect yourself. Check out victim stories from fellow Australians who have been stung by scams.

Register for free SCAMwatch email alerts. We'll keep you up to date with what's on the SCAMwatch radar. You can also report scams to the Australian Competition and Consumer Commission (ACCC) and other government agencies through SCAMwatch.

www.scamwatch.gov.au

SCAMwatch is a website run by the ACCC. The aim of SCAMwatch is to provide information to consumers and small business about how to recognise, avoid and report scams. Scams that are reported to SCAMwatch will be analysed by the ACCC.