



Australian  
Competition &  
Consumer  
Commission

# THE LITTLE BLACK BOOK OF SCAMS

A POCKET-SIZED GUIDE TO SPOTTING, AVOIDING  
AND REPORTING CONSUMER FRAUD



**Australian  
Competition &  
Consumer  
Commission**

# **THE LITTLE BLACK BOOK OF SCAMS**

**A POCKET-SIZED GUIDE TO SPOTTING, AVOIDING  
AND REPORTING CONSUMER FRAUD**

Australian Competition and Consumer Commission  
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601  
© Commonwealth of Australia 2012

This work is copyright. Apart from any use permitted by the *Copyright Act 1968*, no part may be reproduced without prior written permission from the Commonwealth available through the Australian Competition and Consumer Commission.

Requests and inquiries concerning reproduction and rights should be addressed to the Director Publishing, Australian Competition and Consumer Commission, GPO Box 3131, Canberra ACT 2601 or by email to [publishing.unit@accc.gov.au](mailto:publishing.unit@accc.gov.au).

ISBN 978 1 921964 74 9

ACCC 02/13\_24005\_494

[www.accc.gov.au](http://www.accc.gov.au)

# Contents

	Introduction	2
	The Scammers' Black List—top 10 scams to avoid	3
1	Advance fee fraud	4
2	Lottery, sweepstakes and competition scams	6
3	Dating and romance scams	8
4	Computer hacking	10
5	Online shopping, classifieds and auction scams	12
6	Banking, credit card and online account scams	14
7	Small business scams	16
8	Job and employment scams	18
9	Golden opportunity and gambling scams	20
10	Charity and medical scams	22
	Scam delivery methods	24
	The scammers' tool box	27
	Beware the personal touch	28
	The Golden Rules—top 10 tips to protect yourself	29
	Report a scam and more information	30

# Introduction

Every year, scams cost Australians, businesses and the economy millions of dollars, as well as considerable non-financial harm.

This pocket-sized edition of *The Little Black Book of Scams* is brought to you by the Australian Competition and Consumer Commission (ACCC), the national consumer protection agency. *The Little Black Book of Scams* is recognised internationally as an important tool for consumers and small businesses to learn about scams including:

- the most common scams to watch out for
- how scams are delivered
- the tools scammers use to trick you
- personalised scam approaches
- golden rules to protect yourself, and
- where to report a scam.

*The Little Black Book of Scams* is available online at [www.accc.gov.au/littleblackbookofscams](http://www.accc.gov.au/littleblackbookofscams).

## Protect yourself—sign up to SCAMwatch

To stay one step ahead of scammers, visit the ACCC's SCAMwatch website—[www.scamwatch.gov.au](http://www.scamwatch.gov.au)—where you can sign up for free email alerts on new scams targeting consumers and small businesses. You can also follow SCAMwatch on Twitter at @scamSCAMwatch\_gov or [http://twitter.com/SCAMwatch\\_gov](http://twitter.com/SCAMwatch_gov).

# The Scammers' Black List

## —top 10 scams to avoid

These days, scams come in all shapes and sizes. Have you received an offer that seems too good to refuse? Perhaps a request to help someone in a fix or donate to a good cause? Or even an invitation to 'befriend' or connect with an online admirer? Scammers know how to press your buttons to get what they want.

Scammers are increasingly sophisticated in their activities, moving with the times to take advantage of new technology, communications methods, emerging products or services and major events to create plausible stories that will convince you to part with your money or personal details.

However, thanks to the thousands of scam reports received every year, the ACCC has prepared **The Scammers' Black List** to help you identify and avoid the 10 most common methods that scammers use to get at you.

# Advance fee fraud

If you are asked to provide payments in advance to receive goods or money, think twice.

## How the scam works

Advance fee fraud is the most common scam around, accounting for more than half of the scams reported to the ACCC. It includes any scam where a scammer requests fees upfront or personal information in return for goods, services, money or rewards that they never supply. Scammers invent convincing and seemingly legitimate reasons for requesting payment such as to cover fees or taxes. They often ask for payment via international wire transfer. These scams are commonly mass-marketed, with scammers sending them out simultaneously to thousands of people all over the world—usually by mail or email.

The **upfront payment scam** is the most common version of advance fee fraud and involves a scammer promising you a share in money or goods in return for upfront payments or personal information. The promise is never delivered upon. The **Nigerian 419 scam** is the best known example: a scammer offers you a reward in exchange for helping transfer money overseas—all you have to do is give your bank account details and pay fees or taxes. The **fake inheritance scam**, where a scammer claims that you have been left a huge inheritance from a long-lost relative, is also common.

If you fall for advance fee fraud, you will never receive the promised benefit and lose any money you sent.

Other common types of advance fee fraud include **lottery, sweepstakes and unexpected prize scams, dating and romance scams**, and **classifieds scams**. Read on to find out more.



## Protect yourself

- Avoid arrangements with strangers requesting upfront payment via money order, wire transfer or international funds transfer. It's rare to recover money sent this way.
- Conduct a search online using the exact wording of the offer to check if it is legit—many scams can be identified this way.
- Don't open suspicious or unsolicited emails—just delete them.

Money laundering is a criminal offence: do not agree to transfer money for a stranger as you may be helping conceal the source of illegally obtained money.



# Lottery, sweepstakes and competition scams

Don't be lured by a surprise win—only the scammer takes home a windfall.

## How the scam works

These scams try to trick you into giving money upfront or your personal details in order to receive a prize from a lottery, sweepstake or competition that you never entered. Scammers typically claim that you need to pay fees or taxes before your 'winnings' or prize can be released. You may also have to call or SMS a premium rate phone number to claim your prize.

If you pay, you will never receive the promised prize and lose every cent that you send. You may also be up for a hefty phone bill if you called a premium number to collect your prize. If you have provided personal details, your identity could be misused too.

Don't be fooled—scammers use official-looking documents and brochures that appear to have government approval or to have come from a reputable company in order to get under your radar.





---

## Protect yourself

- Remember: you cannot win money in a lottery or competition unless you entered, or someone else did so on your behalf. Tickets in genuine overseas lotteries can only be bought in that country.
- A legitimate lottery does not require you to pay a fee to collect winnings—conduct a search online using the exact wording of the offer to check if it is legit.
- Think twice before calling or text messaging a phone number starting with '19'—they are charged at premium rates.

# Dating and romance scams

Don't let love byte you online.

## How the scam works

Dating and romance scams can cause significant financial and non-financial harm to victims. Financial losses are often quite high, and victims also experience emotional distress when they realise what has happened.

The most common dating and romance scams involve scammers creating fake profiles on legitimate dating websites. They use these profiles to try and enter into a relationship with you so they can get a hold of your money and personal details. The scammer will develop a strong rapport with you then ask for money to help cover costs associated with illness, injury, travel costs or a family crisis. Scammers seek to exploit your emotions by pulling on your heart strings.

These scams may be operated by experienced criminal networks and can run for months or even years. Victims are often approached on legitimate dating websites but the scammer is quick to move the communication away from the security of the website.





---

## Protect yourself

- Never send money or give your personal details to someone you met online even if they tell a convincing tale of woe and ask for your support.
- Avoid any arrangement with a stranger who asks for upfront payment via money order, wire transfer or international funds transfer—it's rare to recover money sent this way.
- Watch out if an online admirer asks to communicate outside the dating website after only a few 'contacts' or conversations—it could be a scammer.

# Computer hacking

If your computer's security is compromised, you are too.

## How the scam works

These days computers are an indispensable part of our lives. The details stored on computers are often very personal, making them valuable to scammers.

**Phishing emails** are commonly used by scammers to trick you into giving them access to your computer. They 'fish' for your personal details by encouraging you to click on a link or attachment. If you click, malicious software will be installed and the hacker will have access to files and information stored on your computer. A phishing email often appears to come from an organisation that you know and trust like a bank or financial institution.

**Social networking scams** can be initiated via a phishing email that asks you to enter your account password on a fake copy of the networking site's login page. If you provide your account details, the scammer can hack in to your account and take control of your profile. They may then pose as you in an attempt to gain money or personal details from your friends, family or followers.

Be on guard offline too—scammers have been known to call you at home and claim that your computer is infected with a non-existent virus or is experiencing technical issues. They will try to convince you to buy fake antivirus software and to give them remote access to your computer. If you buy the software or grant access, the scammer can install malware and spyware to collect your personal details.



Remember: smartphone and tablet devices are computers too.

---

## Protect yourself

- Always keep your computer security up-to-date with anti-virus and anti-spyware software, and a good firewall—only buy software from a reputable source.
- Be cautious if you receive an email or phone call out of the blue claiming to be from a well-known company—use their official contact details to check the call or email is legit.
- Never click on links or open attachments in an email from an unverified sender.

# Online shopping, classifieds and auction scams

Scammers love the ease of online shopping too.

## How the scam works

Consumers and businesses are increasingly buying and selling online. Unfortunately, scammers like shopping online for victims too.

**Not getting what you paid for** is a common scam targeting online shoppers. A scammer will sell a product and send a faulty or inferior quality item, or nothing at all. They may also pretend to sell a product just to gather your credit card or bank account details.

An **online auction scam** involves a scammer claiming that you have a second chance to buy an item that you placed a bid on because the winner has pulled out. The scammer will ask you to pay outside of the auction site's secure payment facility; if you do, your money will be lost and the auction site will not be able to help you.

The **online classifieds scam** is a common scam targeting both buyers and sellers. Buyers should beware of scammers who post fake ads on legitimate classifieds websites. The ads can be for anything from rental properties to pets, used cars or cameras, and will often be cheaply priced. If you show interest in the item, the scammer may claim that they are travelling or have moved overseas and that an agent will deliver the goods following receipt of payment. Following payment you will not receive the goods or be able to contact the seller.

For sellers, a classified scammer will respond to your advertisement with a generous offer. If you accept it, the scammer will pay by cheque or money order. However, the amount that you receive is for more than the agreed price. The 'buyer' may tell you that the overpayment was a



mistake and will ask you to refund the excess amount by money transfer. The scammer hopes that you will transfer the money before you discover that their cheque has bounced or that the money order was phony. You will lose the money, as well as the item you sold if you have already sent it.

---

## Protect yourself

- Before you shop online, do some research to check if the seller is reputable and what protection the website offers against fraud.
- Only pay via the website's secure payment method—look for a web address starting with 'https' and a closed padlock symbol.
- Never accept a cheque or money order for payment that is more than what you agreed upon.



# Banking, credit card and online account scams

Keep your financial details secure and your money safe.

## How the scam works

Your financial details are invaluable to scammers and can be used to commit fraud 24/7 anywhere in the world.

**Phishing scams** are a popular method used to gain your financial details. Scammers send emails or SMS messages that appear to be from your bank, a financial institution or an online payment service. They usually claim that there is a problem with your account and request that you verify your details on a fake but convincing copy of the bank's website.

**Card skimming** is the copying of information from the magnetic strip of a credit card or ATM card. Scammers skim your card by putting a discreet attachment on an ATM or EFTPOS machine. They may even install a camera to capture your pin. Once your card is skimmed, scammers can create copies and make charges to your account.

**Card-not-present fraud** is where scammers use your credit card number and details to pay for a product or service without them physically having your card. Scammers can run up a hefty credit bill buying products online or via the phone.

Be on guard: if a scammer is successful in obtaining your financial details, they can use it to access your money, or commit identity theft or fraud.



---

## Protect yourself

- If you receive an unexpected email, call or SMS from your bank or financial institution, don't provide your personal or financial details. Check the contact is legit—contact the organisation using their official customer service details.
- When you are banking online, check that the web address is correct and the site is not a fake. Make sure the site is secure—look for a web address beginning with 'https' and a closed padlock symbol.
- If you think that your banking or financial details have been compromised, contact your financial institution immediately.

# Small business scams

Scammers take advantage of the busy nature of many small businesses to swindle them.

## How the scam works

Scams targeting small businesses come in all sorts of guises.

A **false billing scam** is the most common trick scammers use against small businesses. Scammers issue fake bills for unwanted or unauthorised listings, advertisements, products or services. The **business directory scam** is a well-known example, where you receive a bill for a listing in a supposedly well-known directory. Scammers trick you to sign up by disguising the offer as an outstanding invoice or a free entry, but with a hidden subscription agreement in the fine print.

The **domain name scam** is another ploy used by scammers, where you are deceived into signing up for an unsolicited internet domain registration very similar to your own. You may also receive a fake renewal notice for your actual domain name and pay without realising.

An **office supply scam** involves you receiving and being charged for products that you did not order. These scams often involve products or services that you regularly order such as stationery and cleaning supplies. Scammers typically call your business pretending that a service or product has already been ordered.

A **fax back scam** is where a scammer faxes you an offer that you have to fax back to a premium rate number (starting with '19') to accept. The scammer then makes sure that it takes several minutes to process the fax, resulting in a hefty phone bill.



Watch out: scammers are especially likely to strike during busy times of the year—for example, the end of financial year.

## Protect yourself

- Don't agree to offers or deals straight away—always ask for an offer in writing and seek independent advice if the deal involves money, time or a long-term commitment.
- Never provide your business' banking, financial and accounting details to someone that contacts you unexpectedly and that you don't know and trust.
- Effective management procedures can go a long way towards preventing scams—have a clearly defined process for verifying and paying accounts and invoices.

# Job and employment scams

Big income—guaranteed? Unlikely!

## How the scam works

Job and employment scams involve offers to work from home or set up and invest in a 'business opportunity'. Scammers promise a job, high salary or large investment return following initial upfront payments. These payments may be for a 'business plan', training course, software, uniforms, security clearance, taxes or fees. These scams are often promoted through spam email or advertisements in well-known classifieds (including websites).

Sometimes you will receive the item but it won't work or be what you expected. Some offers may be a cover for illegal money laundering activities, where you are asked to receive payments into your bank account for a commission and then pass the money on to a foreign company.

Be very wary if you receive an offer to participate in a scheme that requires you to recruit people—it could be a pyramid scheme. Find out more on page 20.





## Protect yourself

- Beware of offers or schemes claiming to guarantee income or requiring payment upfront. Never agree to an offer over the phone—ask for it in writing.
- Do your research before agreeing to any offer—ask around, search online and check if the company is licensed using ASIC's Australian Financial Services licensee register.
- Remember: there are no shortcuts to wealth—the only people that make money are the scammers.

Many work-from-home scams are fronts for money-laundering or pyramid schemes – both are illegal forms of activity in Australia

# Golden opportunity and gambling scams

‘Risk-free investment’ opportunity or opportunity for misfortune?

## How the scam works

If you are looking for a fast way to make money, watch out—scammers are too, and they have invented all sorts of tricks to get you to part with your money.

**Investment opportunity scams** often begin with a phone call or email out of the blue from a scammer offering a ‘not-to-be-missed’, ‘high return’ or ‘guaranteed’ investment in shares, real estate, options or foreign currency trading. While it may seem convincing, in reality the scammer will take your money and you will never receive the promised returns.

A **computer prediction software scam** promises to accurately predict the results of horse races, sports events, stock market movements or lotteries. Scammers promise you huge returns based on past results and trends. In order to participate, you may be asked to pay for membership fees, special calculators, newsletter subscriptions or computer software programs.

**Pyramid schemes** trick you into paying large upfront joining or membership fees to participate in money-making ventures where you have to convince other people to join. People are often persuaded to join by family members or friends. These schemes work by recruiting people rather than selling a legitimate product or service. There is no guarantee that you will recoup your initial investment and, in the end, all pyramid schemes collapse. Pyramid schemes are illegal in Australia.



Watch out: these scams are often highly sophisticated and hard to tell apart from genuine offers. If you sign up for one, you will lose your money.

## Protect yourself

- Do your research before signing up to an investment or money-making offer that promises amazing returns—ask around, search online and check if the company is licensed using ASIC's Australian Financial Services licensee register.
- Ask yourself: If a stranger knew a secret to making money, why would they share it?
- Remember: there are no get-rich-quick schemes—the only people who make money are the scammers.



# Charity and medical scams

Charitable and health conscious consumers beware—scammers will try anything to get your money.

## How the scam works

Scammers are unscrupulous and do not hesitate to take advantage of people seeking to donate to a good cause or find an answer to a health problem.

**Charity scams** involve scammers collecting money by pretending to work for a legitimate cause or charity, or a fictitious one they have created. Often scammers will exploit a recent natural disaster or crisis that has been in the news. They may also play on your emotions by claiming to collect for a cause that will secure your sympathy, for example to help sick children.

These scams divert much-needed donations away from legitimate charities and causes. Charities must be registered with government—donate confidently by checking their registration first.

**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 are often promoted using false testimonies from people who 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, a ‘fat-busting’ device, breakthrough pills, patches or creams. You may be required to make a large advance payment or enter into a long-term contract to receive ongoing supplies.



**Fake online pharmacies** offer counterfeit drugs and medicine at very cheap prices, and sometimes provide them without a doctor's prescription. These drugs may have limited or no active ingredients, which can have lethal consequences for users.

---

## Protect yourself

- If you have been approached to make a donation, first contact the charity directly and check their government registration.
- Consult your healthcare professional if you are considering a 'miracle' or 'instant-fix' claim about medicines, supplements or other treatments.
- Ask yourself: if this really is a miracle cure, wouldn't your healthcare professional have told you about it?

# Scam delivery methods

Scammers are increasingly sophisticated in how they approach you, taking advantage of new technology and communication methods to try and get under your radar. Here are some of the most common delivery methods that scammers use.

## Online

The internet breathes new life into old scams and generates fresh ones too

**Email services** are a favoured scammer's delivery method, providing a free and easy way to communicate en masse and also one-on-one with potential victims. Phishing emails that 'fish' for your personal information are the most common email scam type.

**Social networking platforms** offer scammers the chance to 'befriend' you and enter your personal life to access your personal details, which can then be used against you, your family and friends.

**Online shopping, classifieds and auction sites** are used by scammers to target buyers and sellers, with initial contact often made through reputable and trusted sites before being moved away from the site's security and payment facilities.

**Online money transfers services**, including wire transfer or international funds transfers, are commonly used by scammers as they allow money to be transferred overseas very quickly. It is rare to trace or recover money sent this way.



## Over the phone

### Scammers call and SMS too

**Phone calls** are made by scammers to homes and businesses in an attempt to get you to fall for whatever scam they are pedalling. This type of direct delivery method allows scammers to develop a rapport with you and play on your emotions to get the desired effect.

**SMS text messages** are used by scammers to send competition or prize scams. Scammers often try to snare many people with one SMS—this is known as spamming. If you respond, you may be charged at premium rates or find yourself signed up to a subscription service.

**Smartphone and tablet devices** are the portal for the next generation of malware scams, with scammers hiding malicious software in downloads such as applications, attachments or games. Once on your device, the software can steal your personal information.

**Faxes** are also used by scammers to target small businesses with amazing offers in the hope that you will fax back to a premium rate service number, resulting in a hefty phone bill.



## At your door

Watch out—some scammers will come right to your door to try and scam you

**Door-to-door scams** usually involve the scammer promoting goods or services that are not delivered or are of a very poor quality. You may even get billed for work that you did not want or agree to. A common door-to-door scam is carried out by dodgy itinerant traders who move through regional centres and do shoddy home repairs or just take your money and run.

Many legitimate businesses use door-to-door selling to approach you. You have specific rights when it comes to door-to-door sales practices including when payment is required and the chance to change your mind—find out more at [www.accc.gov.au/doortodoor](http://www.accc.gov.au/doortodoor).

**Postal services** also continue to be used by scammers to deliver scams including fake **lottery and sweepstake letters**, **chain letters** and fake **inheritance letters**. Scammers have also been known to pretend to be legitimate postal service providers and ask for money to deliver parcels.



# The scammers' tool box

Scammers have a large tool box of tricks at their disposal to snare you. Here is a list of common tools used.

- **Not-so-tall tales:** scammers spin elaborate, yet convincing yarns to get what they want.
- **Information harvesting:** scammers invest a lot of time and money collecting information on potential victims from public listings, black market lists or even directly from you.
- **Counterfeit and official-looking documents:** a document that appears to have government approval can give a scam an air of authenticity.
- **Mirror and fake websites:** it's easy for scammers to copy a legitimate website and use a slightly different web address to trick you.
- **Whiz-bang gadgets and offers:** scams can come with all sorts of enticements including discounts, deals, special calculators, computer software and magazine subscriptions.
- **High pressure sales tactics:** scammers know how to up the ante to create a sense of excitement, anxiety or fear.
- **Phishing:** scammers send emails or SMS to 'fish' for and collect your personal details.
- **Malicious software:** scammers use this to hack your computer via infected links, attachments, downloads or fake pop-up alerts.
- **Victims lists:** scammers buy lists containing the details of people who have previously fallen for a scam in order to try and trick them again.
- **Business fronts:** a scam can have all the hallmarks of a professional business model including physical or virtual offices, call centres and administrative procedures.
- **International money wires or transfers:** an easy way for scammers to collect money and evade detection.

# Beware the personal touch

## Scammers will do anything to target you, including adopting a personal touch

Scammers have realised that one of the best ways to fool you into falling for a scam is to make it personal. Your personal details are the scammers' key to making a scam appear legitimate as they can tailor it to you based on who you know, what you do and your personal interests.

**Impersonation** of well-known and trusted government bodies, organisations and companies is being used more and more by scammers when they approach you. Scammers misuse our trust in such entities by claiming to represent them in person or via visual tricks such as copying logos, letterheads and websites.

**Spear and whale phishing** are emails that specifically target organisations or senior executives with the hope of gaining confidential company information, passwords or banking details.

**Grooming victims** is another ploy used by scammers to build a trusting relationship with victims via regular contact. Groomers aim to extract greater amounts of money or personal information than they could have via a one-off contact. They will try convincing you that they are your friend or, in some cases, a romantic interest.

**Playing on your emotions** is another method that scammers use to slip under your radar. Scammers will not hesitate to appeal to your charitable side, make an urgent plea for help, pretend that danger is imminent, or claim to be in love with you—all to create a sense of guilt, anxiety, fear or personal attachment that will push you to fall for their scheme.

Personalised scams can result in significant non-financial harm to victims such as adverse affects to their mental and physical health, work capacity, relationships and family.

# The Golden Rules—top 10 tips to protect yourself

Follow the 10 Golden Rules to protect yourself from scams.

1. **Watch out for scams**—scammers target you anytime, anywhere, anyhow.
2. **Don't respond**—ignore suspicious emails, letters, house visits, phones calls or SMS messages—press 'delete', throw them out, shut the door or just hang up.
3. **Don't agree to an offer straight away**—do your research and seek independent advice if it involves significant money, time or commitment, and get the offer in writing.
4. **Ask yourself who you're really dealing with**—scammers pose as people or organisations that you know and trust.
5. **Don't let scammers push your buttons**—scammers will play on your emotions to get what they want, including adopting a personal touch.
6. **Keep your computer secure**—always update your firewall, anti-virus and anti-spyware software, and only buy from a verified source.
7. **Only pay online using a secure payment service**—look for a URL starting with 'https' and a closed padlock symbol.
8. **Never send money to someone you don't know and trust**—it's rare to recover money from a scammer.
9. **Protect your identity**—your personal details are private and invaluable; keep them that way and away from scammers.
10. **If you've spotted a scam, spread the word!**—tell your family and friends, and report it to SCAMwatch—[www.scamwatch.gov.au](http://www.scamwatch.gov.au).



# Report a scam and more information

If you think you have spotted a scam or have been scammed, there are many government agencies in Australia that you can contact for advice or to make a report. The best agency to contact depends on where you live and what type of scam is involved.

## Scams from interstate or overseas

### **The Australian Competition and Consumer Commission (ACCC)**

The ACCC is Australia's national consumer protection agency and can give you information and advice on what to do if you have spotted a scam or been scammed.

The ACCC runs SCAMwatch, the Australian Government's website for information on scams. Use the SCAMwatch report a scam form to lodge a report online.

- SCAMwatch Infocentre: 1300 795 995
- SCAMwatch website: [www.scamwatch.gov.au](http://www.scamwatch.gov.au)
- SCAMwatch Twitter: @scamwatch\_gov or [http://twitter.com/SCAMwatch\\_gov](http://twitter.com/SCAMwatch_gov).

### **econsumer.gov**

An initiative of the International Consumer Protection and Enforcement Network, econsumer.gov receives complaints about online and related transactions with foreign companies and helps cross-border enforcers spot fraud trends.

- [www.econsumer.gov](http://www.econsumer.gov)

## Local scams

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

### **New South Wales Fair Trading**

- 13 3220
- [www.fairtrading.nsw.gov.au](http://www.fairtrading.nsw.gov.au)
- ScamBuster mobile app—free to download at [www.fairtrading.nsw.gov.au](http://www.fairtrading.nsw.gov.au)

### **Consumer Affairs Victoria**

- 1300 558 181
- [www.consumer.vic.gov.au](http://www.consumer.vic.gov.au)

### **Queensland Office of Fair Trading**

- 13 7468
- [www.fairtrading.qld.gov.au](http://www.fairtrading.qld.gov.au)

### **Consumer and Business Services in South Australia**

- 13 1882
- [www.ocba.sa.gov.au](http://www.ocba.sa.gov.au)

### **Western Australia Department of Commerce**

- 1300 304 054
- [www.commerce.wa.gov.au](http://www.commerce.wa.gov.au)
- WAScamNet—subscribe to receive scams alerts in WA at [www.scamnet.wa.gov.au](http://www.scamnet.wa.gov.au)

### **Australian Capital Territory Office of Regulatory Services**

- 02 6207 3000
- [www.ors.act.gov.au](http://www.ors.act.gov.au)

## **Northern Territory Consumer Affairs**

- 1800 019 319
- [www.consumeraffairs.nt.gov.au](http://www.consumeraffairs.nt.gov.au)

## **Tasmania Consumer Affairs and Fair Trading**

- 1300 654 499
- [www.consumer.tas.gov.au](http://www.consumer.tas.gov.au)

## **Financial and investment scams**

### **The Australian Securities and Investments Commission (ASIC)**

ASIC is Australia's corporate, markets and financial services regulator and can give you information and advice on what to do if you have spotted a scam or been scammed in relation to financial products and services.

ASIC runs MoneySmart, the Australian Government's website to help you make better financial decisions. Use the MoneySmart report a scam form to lodge a report online.

- 1300 300 630
- MoneySmart website: [www.moneysmart.gov.au](http://www.moneysmart.gov.au)

## **Banking and credit card scams**

### **Your bank or financial institution**

If you think you have received a scam about your account, let your bank or financial institution know. If your account details have been compromised, alert them immediately.

In some cases your bank may be able to reverse an unauthorised credit card charge for a transaction that was not fulfilled.

## Spam email and SMS

### **The Australian Communications and Media Authority (ACMA)**

The ACMA is Australia's regulator for broadcasting, the internet, radio and telecommunications, and can give you information and advice on what to do if you have received spam via email or SMS.

- 1300 850 115
- [www.acma.gov.au](http://www.acma.gov.au)
- Spam email—forward on to: [report@submit.spam.acma.gov.au](mailto:report@submit.spam.acma.gov.au)
- Spam SMS—forward on to: 0429 999 888

## Fraud, theft and other crimes

### **Your local police**

Many scams may breach the fraud provisions of various crime acts such as identity fraud or theft. If you think you have been defrauded, you should contact your local police station. If you have been threatened, assaulted or had your property stolen, contact the police immediately.

### **Victims' Certificate**

If your identity has been compromised, you may be able to apply for a Victims' Certificate to assist you in overcoming problems in your personal and business affairs caused by that crime—contact the Australian Government Attorney-General's Department for more information.

- <http://www.ag.gov.au/victimscertificates>

## More information

The Australian Government has some great resources on how stay secure and safe online.

- Stay Smart Online Service—[www.staysmartonline.gov.au](http://www.staysmartonline.gov.au)
- CyberSmart website—[www.cybersmart.gov.au](http://www.cybersmart.gov.au)
- *Protecting Yourself Online* publication—available at [www.ag.gov.au/cybersecurity](http://www.ag.gov.au/cybersecurity)

## SCAMwatch

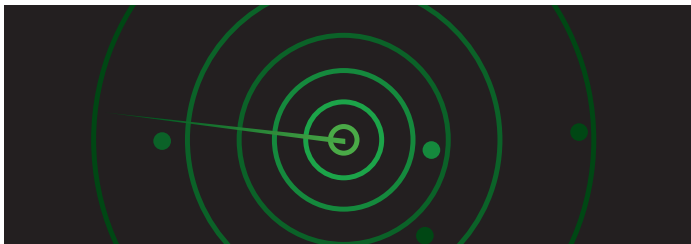
### Don't let scams sneak under your radar!

Stay one step ahead of the scammers—visit the SCAMwatch website to get the low-down on scams that target Australian consumers and small businesses. Find out more about how scams work, how to protect yourself and what to do if you've been scammed.

Register with the SCAMwatch subscription service to receive free email alerts on new scams doing the rounds.

**[www.scamwatch.gov.au](http://www.scamwatch.gov.au)**

Follow SCAMwatch on Twitter at [@scamwatch\\_gov](https://twitter.com/scamwatch_gov) or [http://twitter.com/SCAMwatch\\_gov](http://twitter.com/SCAMwatch_gov).



[www.scamwatch.gov.au](http://www.scamwatch.gov.au)

