AUSTRALIAN COMPETITION & CONSUMER COMMISSION

The Little Black Book of Scams

A pocket-sized guide so you can spot, avoid, and protect yourself against scams

The Little Black Book of Scams

A pocket-sized guide so you can spot, avoid, and protect yourself against scams

ISBN 978 1 920702 00 7

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

ACCC 12/16_1129

www.accc.gov.au

Contents

Introduction

Every year, scams cost Australians, businesses and the economy hundreds of millions of dollars and cause emotional harm to victims and their families.

The best way to protect yourself is through awareness and education. This new 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
- the different ways scammers can contact you
- the tools scammers use to trick you
- the warning signs
- how to protect yourself, and
- where you can find help.

The Little Black Book of Scams is available online at www.accc.gov.au/littleblackbookofscams.

Protect yourself—sign up to Scamwatch

To stay one step ahead of scammers, learn more by visiting the ACCC's Scamwatch website—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 @scamwatch_gov or http://twitter.com/scamwatch_gov.

The top scams to avoid

Everyone is vulnerable to scams so everyone needs information about how to identify and avoid being scammed. Some people think that only the gullible and greedy fall victim to scams. The truth is scammers are clever and if you don't know what to look out for, anyone can fall victim to a scam.

Have you received an offer that seems too good to be true, perhaps a phone call to help fix your computer or a threat to pay money you do not owe, an alert from your bank or telecommunications provider about a problem with your account or even an invitation to 'befriend' or connect online? Scammers know how to press your buttons to get what they want.

They are getting smarter, moving with the times to take advantage of new technology, new products or services and major events to create believable stories that will convince you to part with your money or personal details.

However, thanks to the tens of thousands of scam reports received every year, the ACCC has prepared a list of common scams to reveal the secrets and tactics that scammers don't want you to know.

Dating and romance scams

Dating and romance scams cost Australians millions every year and can ruin individuals and families.

How the scam works

Dating and romance scammers create fake profiles on legitimate dating websites, mobile apps or social media platforms like Facebook using photos and identities often stolen from other people. They use these profiles to try to enter into a relationship with you that can run for months or even years, just so they can get a hold of your money. The scammer will ask for money to help with illness, injury, travel costs or a family crisis. They are heartless and will lie to you to take advantage of your better nature.

Scammers will usually be overseas and have an excuse for why they are there, such as being on military service, working as an engineer or caring for a friend or relative. They are never who they say they are and some cunning scammers may even send small gifts. This is only part of their grand plan to get even more money out of you later.

Protect yourself

- Never send money or give your personal details to someone you have only met online.
- Watch out if an online admirer asks to communicate outside the dating website or social media platform after only a few 'contacts' or conversations—it could be a scammer.
- Do an image search of your admirer to help determine if they really are who they say they are. You can use image search services such as Google or TinEye.
- Be cautious when sharing intimate pictures or videos online. Scammers are known to blackmail their targets using pictures or video of you that you don't want anyone else to see.

Investment scams

'Risk-free investment' or opportunity for misfortune?

How the scam works

Investment scams come in many forms including cryptocurrency purchase, binary options trading, business ventures, superannuation schemes, managed funds and the sale or purchase of shares or property. Scammers dress up 'opportunities' with professional looking brochures and websites to mask their fraudulent operations. They 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' opportunity. The scammer usually operates from overseas, and will not have an Australian Financial Services licence.

Computer prediction software scams promise to accurately predict stock market movements, the results of horse races, sports events or lotteries. They are simply a form of gambling disguised as investments. Most of the schemes or programs do not work and buyers cannot get their money back. In many cases the supplier simply disappears.

Superannuation scams offer to give you early access to your super fund, often through a self-managed super fund or for a fee. The scammer may ask you to agree to a story to allow the early release of your money and then, acting as your financial adviser, they will deceive your superannuation company into paying out your super benefits directly to them. Once they have your money, the scammer may take large 'fees' or leave you with nothing at all.

Protect yourself

- Don't let anyone pressure you into making decisions about your money or investments—especially if the offer has come out of the blue.
- Before parting with your money, do your own research on the investment company and check out www.moneysmart.gov.au to see if they have an Australian Financial Services Licence. Ask yourself: if a stranger knew a secret to making money, why would they share it?

If you are under retirement age, watch out for offers promoting easy access to your preserved superannuation benefits. If you illegally access your super early, you may face penalties under taxation law.

Threat and penalty scams

If a government authority or trusted company is telling you to pay up, stop, think and double-check.

How the scam works

Instead of offering a prize, money or rebate, these scams use threats designed to frighten you into handing over your money. The scammer may call you and threaten you with **arrest** or send you an email claiming you owe money for a **speeding fine**, a **tax office debt** or an **unpaid bill**.

During the phone call, scammers will pressure you into paying immediately and tell you the police will be sent to your house if you refuse. Scammers have been known to target vulnerable people in our community, such as newly arrived migrants. They pretend to be Immigration Department officials and threaten victims with **deportation** unless fees are paid to correct errors in their visas. A very similar scam involves the scammer pretending to be from the Australian Tax Office telling their victims they have an outstanding tax bill.

Scammers also pretend to be **trusted companies** such as your bank, gas, electricity, water or phone provider. They will threaten to cancel your service or charge you excessive penalty fees if you don't pay the bill immediately. Sometimes they may impersonate a business like Australia Post stating you have an item to pick up or you will be charged a holding fee every day you don't pay. Whatever the case, they try to make you worried and act without stopping to think and check that the story is true.

If the scam is sent by email, it is likely to include an attachment or link to a fake website where you will be asked to download proof of the 'bill', 'fine' or 'delivery details'. Opening the attachment or downloading the file will result in infecting your computer with malware (see page 16).

Protect yourself

- Don't be pressured by a threatening caller. Stop, think and check whether their story is true.
- A government agency or trusted company will never ask you to pay by unusual methods such as by gift card, wire transfers or Bitcoins.
- Verify the identity of the contact by calling the relevant organisation directly—find them through an independent source such as a phone book, past bill or online search.
- Do not use the contact details provided in emails or given to you during phone calls. Again, find them through an independent source.

Unexpected money scams

If you are asked to provide payments before receiving goods or money, think twice.

How the scam works

Scammers tell you out of the blue that you are entitled to money, precious gems, gold or valuable shares but you need to make **upfront payments** to get them. You will never receive what was promised and there will always be an excuse for why you have to pay more. If you pay the fees, you will lose your money.

Rebate or reclaim scams involve a scammer telling you that you are owed money for reasons such as overpaid taxes, bank fees or some sort of compensation. However, before you can get your money you are asked to pay a small administration fee.

With **inheritance scams**, scammers pose as lawyers, bankers or foreign officials and tell you that you are entitled to a large inheritance or offer you a share in a scheme because you have the same name as someone who died. They often use official-looking documents and ask you to make payments for fees and taxes before you can receive the inheritance. They can also ask for your personal details to fill out 'official paperwork'. This means that you might have your identity stolen as well as your money.

Commonly called **Nigerian scams** may have originated in West Africa but can come from anywhere in the world. They involve scammers

telling you they need your help to secure a large fortune which they are desperately trying to transfer out of their country. They may claim the fortune is a hidden stash of money, gold or assets abandoned by a corrupt government or official and if you agree to receive it they will give you a large share when it is safe to do so. Like all of these scams, they will say you first need to pay taxes, bank charges or fees for anti-terrorism and money laundering checks before they can send the money.

These scams commonly come from overseas and ask for payment via wire transfer but may also ask for bank transfers or other payment methods.

If you fall for these scams, you will never receive anything from the scammer and lose any money you sent.

Protect yourself

- Remember there are no get-rich-quick schemes: if it sounds too good to be true it probably is.
- Avoid any arrangement with a stranger that asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. It is rare to recover money sent this way.
- If an unsolicited email looks suspicious, just delete it. Don't click on any links.
- Government departments, banks or utilities will never contact you asking you to pay money upfront in order to claim a fee or rebate.
- If you are unsure, check the identity of the contact independently. Do not use the contact details provided in the message sent to you—get correct contact details through an independent source such as a phone book or online search.
- Conduct a search online using the exact wording of the offer—many scams can be identified this way.

Prize and lottery 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 claim that you need to pay fees or taxes before your 'winnings' or prize can be released. You may also have to call or send a text to a premium rate phone number to claim your prize.

Scratchie scams involve getting mail containing glossy brochures and a number of scratchie cards, one of which will be a winner. To make it more believable, it will often be second or third prize. When you call to claim your prize, the scammers will ask for fees or taxes to be paid before you can get your winnings.

Lottery scams may use the names of real overseas lotteries to claim that you've won cash, even though you never entered into them. Scammers normally ask for fees or taxes to release the funds. They will also tell you they need your personal details to prove you are the correct winner but then use this information to steal your identity or money from your bank account.

Fake vouchers and gift cards involve scammers sending you an email or text message or a social media message claiming you have won a gift card for a well-known retailer but you need to provide some details before you can claim it. This is an attempt to get personal information which can be used for identity theft or to target you with another scam. Offers like these have also been known to deliver ransomware on your device (see page 17).

Travel prize scams involve scammers claiming you've won a free holiday or airfares. In fact, what you've actually won is the chance to buy accommodation or flight vouchers. These travel vouchers often have hidden fees and conditions, or may be fake and worthless. Similarly, scammers may offer you amazing discounted holiday packages that just don't exist.

Protect yourself

- Remember: you cannot win money in a lottery or competition unless you entered.
- Competitions and lotteries do not require you to pay a fee to collect winnings—conduct a search online using the exact wording of the offer. It may help confirm that it's a scam.
- Think twice before calling or text messaging a phone number starting with '19'—they are charged at premium rates.

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 to shop online for victims.

Scammers can create very convincing **fake retailer websites** that look like the real thing, including on social media like Facebook. The biggest tip-off that a retail website is a scam is the method of payment – be wary if you are asked to pay by wire transfer or other unusual methods.

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 you won't get what you paid for 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. In this **overpayment scam**, the 'buyer' may tell you that this 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

- Find out exactly who you are dealing with. If it is an Australian retailer, you are in a much better position to sort out the problem if something goes wrong.
- Check if the seller is reputable, has a refund policy and complaint handling services.
- Avoid any arrangement that asks for up-front payment via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. It is rare to recover money sent this way. Never send money or give credit card or online account details to anyone you don't know or trust and never by email.
- 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 or forward money on for anyone.

Scams targeting computers and mobile devices

Remember: anything that connects to the internet is vulnerable.

How the scam works

Remote access scammers call you on the phone claiming that your computer is infected by viruses. If you follow their instructions, it will allow them to access and control your computer where they can steal information or install malware. They may also try to convince you to purchase 'anti-virus' software, which usually turns out to be overpriced or freely available on the internet.

Malware is a term for any malicious software that can be installed on your computer or other devices including viruses, spyware, ransomware, trojan horses and keystroke loggers.

Keystroke loggers and spyware allow scammers to record exactly what you type on your keyboard to find out passwords and bank details or access personal information and send this anywhere they want. Once installed, scammers can control your email and social media accounts and grab whatever information is on your device, including passwords. They can also use your accounts to send more scams to your friends and family.

Ransomware is another type of malware that encrypts or locks your device to prevent you from using it until a payment is made to unlock it. Paying up doesn't guarantee it will be unlocked or be free from hidden viruses, which can also spread and infect other computers or devices on your network.

Malware is commonly delivered by email and can appear to be from legitimate sources, such as your utility provider, a government agency or even the police purporting to issue a fine. Don't click on the link or open any attachments that you aren't absolutely sure about. You may be downloading malicious software instead. These scams target both individuals and businesses.

Protect yourself

- Be wary of free downloads offering music, games, movies and access to adult sites. They may install harmful programs without you knowing.
- Keep your office networks, computers, and mobile devices secure. Update your security software, change passwords and back up your data regularly. Store your backups offsite and offline. www.staysmartonline.gov.au explains how to back-up your data and secure your mobile devices.
- Do not open attachments or click on links in emails or social media messages you've received from strangers—just press delete.

Identity theft

All scams have the potential for identity theft. Protecting yourself from scams also means keeping your personal information safe.

Identity theft is a threat in every scam

Most people associate scams with attempts to trick you out of your money. However, your information is also valuable to scammers. Scammers steal your personal details to commit fraudulent activities like making unauthorised purchases on your credit card, or using your identity to open bank or telephone accounts. They might take out loans or carry out other illegal business under your name. They may even sell your information to other scammers for further illegal use.

Having your identity stolen can be both financially and emotionally devastating. It can take months to reclaim your identity and the impact of having it stolen can last for years.

Phishing—a scammer contacts you out of the blue via email, phone, Facebook or text message pretending to be from a legitimate business such as a bank, phone or internet service provider. They direct you to a fake version of the business's website asking for your personal details to verify customer records due to a technical error. They may call imitating a luxury goods retailer claiming that someone is trying use your credit card. They advise you to contact your bank but they don't hang up from their end and keep the line open. When you try to call the bank, you are still talking to

the scammers who simulate a real call, imitate bank staff and ask for your account and security details. In either case, the scammer captures whatever information you give them and then uses it to access your accounts.

Fake surveys—Scammers offer prizes or rewards such as gift cards to well-known retailers in return for completing an online survey. The survey requires you to answer a range of questions including disclosure of important identification or banking details.

As part of any scam—Scammers often ask for personal information in other scams. In a lottery scam, scammers often ask for a driver's licence or passport to 'prove your identity before they can release the prize money'. In dating and romance scams they might ask for information 'to sponsor their visa application to visit you in Australia'.

Remember: Giving away personal information to a scammer can be just as bad as giving away money. Keep your personal details to yourself and keep them secure.

Protect yourself

- **Think twice about what you say and do in an online environment**
  Be careful sharing information about yourself online, including social media, blogs and other online forums. Stop and think before filling in surveys, entering competitions, clicking on links or attachments, or even 'befriending', 'liking' or 'sharing' something online.
- **Beware of any request for your details or money**
  Scammers will try to trick you into handing over your data by using the names of well-known companies or government departments. If you think it's a scam, don't respond. Use the phone book or an online search to check the organisation's contact details. Never use the contact details provided in the original request.

If you have provided personal identification information to scammers, contact IDCARE on 1300 432 273.

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. If you pay the fee you may not receive anything or not what you expected or were promised.

Some job offers may be a cover for **illegal money laundering** activities, where you are asked to act as an 'accounts manager' or 'personal assistant', receive payments into your bank account for a commission, and then pass the money on to a foreign company.

Job scams are often promoted through spam email or advertisements in well-known classifieds and on job seeker websites—even government job seeker websites.

A big danger with these job scams is that you can be asked for a lot of personal details that you should not provide including your tax file number and copies of your passport or driver's licence. This information could be used later for identity theft.

Protect yourself

- Beware of offers or schemes claiming to guarantee income or requiring payment upfront.
- Never agree to transfer money for someone else—this is money laundering and it is illegal.
- Do not provide your tax file number, driver's licence or passport when applying for a job. You may need to provide this information but only after you have started work.

Money laundering is a criminal offence: do not agree to transfer money for a stranger.

Charity and medical scams

Scammers are heartless and can strike during desperate times of need.

How the scam works

Scammers 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.

These scams divert much-needed donations away from legitimate charities. 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 are approached by a charity street collector, ask to see their identification. If you have any doubts about who they are, do not pay.
- Check the Australian Charities Not for Profit Association's list of registered charities.
- 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?

Business scams

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

How the scam works

Scams targeting businesses come in all sorts of guises and are likely to strike at the busiest times, like the end of the financial year.

A **false billing scam** is the most common trick scammers use against 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 listing, 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.

Payment redirection scams involve a scammer using information they have obtained by hacking your computer systems. They then pose as one of your regular suppliers and tell you that their banking details have changed. They may tell you they have recently changed banks, and may use copied letterhead and branding to convince you they are legitimate. They will provide you with a new bank account number and ask that all future payments are processed accordingly. The scam is often only detected when your regular supplier asks why they have not been paid.

Ransomware can be extremely damaging for any business. The best defence is to back up your data regularly and store your backups offsite and offline. See more detail at page 17.

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 clearly defined processes for verifying and paying accounts and invoices and look very carefully at requests to change banking details.
- Train your staff to recognise scams.
- Back up your business data offsite and offline.
- Beware of emails requesting changes to payment details. Always verify changes to payment details directly with the business or individual.

How scams work—the anatomy of a scam

Most scams follow the same pattern and once you understand this, the tricks of the scammer become easier to spot.

If you look carefully at all of the different types of scams outlined in this book, you'll soon notice that most scams go through three stages: (1) approach; (2) communication; and (3) payment.

Understanding the basic parts of a scam will help you to avoid the current crop of scams and to be on guard against new scams that emerge in the future.

1. The approach: delivery method

When scammers approach you it will always come with a story designed to make you believe a lie. The scammer will pretend to be something they are not, a government official, an expert investor, a lottery official or even a romantic admirer.

To deliver these lies to you, scammers will use a range of communication methods.

Online

Scammers lurk within the anonymous environment of the internet.

Email is a favoured scam delivery method, providing a cheap and simple way to communicate on a large scale. Phishing emails that 'fish' for your personal information are the most common email scam type.

Social networking platforms, **dating sites and online forums** allow scammers to 'befriend' you and enter into your personal life to access your personal details, which can then be used against you or 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 or fake websites that look like the real thing. Look for secure payment options and beware of unusual payment methods such as wire transfer, Bitcoins or pre-loaded money cards. Credit cards usually offer some protection.

Over the phone

Scammers call and SMS too.

Phone calls are made by scammers to homes and businesses in a wide variety of scams, from threatening tax scams to offers of prizes or 'help' with computer viruses. The availability of cheap Voice Over Internet Protocol (VOIP) telephone calls means call centres can operate offshore with telephone numbers that look like they're local numbers. Telephone caller identification can easily be disguised and is one of the many tricks scammers use to make you believe they are someone else.

SMS text messages are used by scammers to send a whole range of scams including competition or prize scams. If you respond, you may be charged at premium rates or find yourself signed up to a subscription service. It is safer not to respond or click on links in text messages unless you know who they came from. They can also contain attachments or links to malicious software in the guise of photos, songs, games or apps.

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 traders who move from place to place and do shoddy home repairs or just take your money and run.

Legitimate businesses can sell door-to-door but must clearly identify themselves and their company and follow other rules. You have specific rights when it comes to door-to-door sales practices including the chance to change your mind—find out more at www.accc.gov.au/doortodoor.

Scammers can pose as **fake charity** workers to collect donations. They will take advantage of recent events like floods and bushfires. Before donating ask for identification and see their official receipt book.

Bulk mailing is still used to send **lottery and sweepstake scams**, **investment opportunities**, **Nigerian scams** and **fake inheritance letters**. A glossy brochure is no guarantee that an offer is legitimate.

Regardless of the delivery method they use, their story is always the bait and if you bite, the scammer will attempt to move you to the next stage.

2. Communication and grooming

If you give them a chance to talk to you, they will start using tricks in their **scammers' toolbox** to convince you to part with your money.

Scammer's tools can involve the following:

- Scammers spin elaborate, yet **convincing stories** to get what they want.
- They use your **personal details** to make you believe you have dealt with them before and make the scam appear legitimate.
- Scammers may **contact you regularly** to build trust and convince you that they are your friend, partner or romantic interest.
- They **play with your emotions** by using the excitement of a win, the promise of everlasting love, sympathy for an unfortunate accident, guilt about not helping or anxiety and fear of arrest or a fine.
- Scammers love to create a **sense of urgency** so you don't have time to think things through and react on emotions rather than logic.
- Similarly, they use **high pressure sales tactics** saying it is a limited offer, prices will rise or the market will move and the opportunity will be lost.
- A scam can have all the hallmarks of a real business using **glossy brochures** with technical industry jargon backed up with office fronts, call centres and professional websites.
- With access to the internet and clever software it is easy for scammers to create counterfeit and **official-looking documents**. A document that appears to have government approval or is filled with legal jargon can give a scam an air of authority.

The scammer's tools are designed to get you to lower your defences, build trust in the story and act quickly or irrationally and proceed to the final stage—sending the money.

3. Sending the money

Sometimes the biggest clue you will have that it is a scam is the way the scammer asks you to pay.

Asking for money can come within minutes of the scam or after months of careful grooming. Scammers have their preferences for how you send your money.

Scammers have been known to direct victims to their nearest **money remittance** location (post office, wire transfer service or even the bank) to send money. They have been known to stay on the phone, give specific instructions and may even send a taxi to help with this. Scammers are willing to accept money by any means and this can include **direct bank transfers**, **preloaded debit cards**, **gift cards**, **Google Play, Steam, or iTunes cards** or virtual currency such as **Bitcoin**. Any request for payment by an unusual method is a tell-tale sign that it is part of a scam.

Credit cards usually offer some protection and you should also look for secure payment options where 'https' appears in the web address and the site has a closed padlock symbol.

Don't send money to someone you have only met online or over the phone—especially if they are overseas.

Be aware that scammers can also ask for payment in the form of valuable goods and expensive gifts such as jewellery or electronics. Paying money to scammers isn't the only thing you should worry about—if you help transfer money for a stranger you may unwittingly be involved in **illegal money laundering** activities.

The golden rules to protect yourself

Be alert to the fact that scams exist. When dealing with uninvited contacts from people or businesses, whether it's over the phone, by mail, email, in person or on a social networking site, always consider the possibility that the approach may be a scam. Remember, if it looks too good to be true, it probably is.

Know who you're dealing with. If you've only ever met someone online or are unsure of the legitimacy of a business, take some time to do a bit more research. Do a Google image search on photos or search the internet for others who may have had dealings with them.

Do not open suspicious texts, pop-up windows or emails—delete them. If unsure, verify the identity of the contact through an independent source such as a phone book or online search. Don't use the contact details provided in the message sent to you.

Keep your personal details secure. Put a lock on your mailbox and shred your bills and other important documents before throwing them out. Keep your passwords and pin numbers in a safe place. Be very careful about how much personal information you share on social media sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.

Beware of unusual payment methods. Scammers often ask for payment by wire transfers, preloaded cards and even Google Play, Steam, or iTunes cards and Bitcoin. These are nearly always a sign that it is part of a scam.

Keep your mobile devices and computers secure. Always use password protection, don't share access with others (including remotely), update security software and back up content. Protect your WiFi network with a password and avoid using public computers or WiFi hotspots to access online banking or provide personal information.

Choose your passwords carefully. Choose passwords that would be difficult for others to guess and update them regularly. A strong password should include a mix of upper and lower case letters, numbers and symbols. Don't use the same password for every account/profile, and don't share your passwords with anyone.

Beware of any requests for your details or money. Never send money or give credit card numbers, online account details or copies of personal documents to anyone you don't know or trust. Don't agree to transfer money or goods for someone else: money laundering is a criminal offence.

Be careful when shopping online. Beware of offers that seem too good to be true, and always use an online shopping service that you know and trust. Think twice before using virtual currencies (like Bitcoin)—they do not have the same protections as other transaction methods, which means you can't get your money back once you send it.

Where to find help or support

If you've lost money to a scam or given out your personal details to a scammer, you're unlikely to get your money back. However, there are steps you can take straight away to limit the damage and protect yourself from further loss.

Contact your bank or credit union

If you've sent money or personal banking information to a scammer, contact your bank or credit union immediately. They may be able to stop a money transfer or cheque, or close your account if the scammer has your account details. Your credit card provider may be able to perform a 'charge back' (reverse the transaction) if your credit card was billed fraudulently.

Recover your stolen identity

If you suspect you are a victim of identity theft, it is important that you act quickly to reduce your risk of financial loss or other damages.

Contact **IDCARE**—a free, government-funded service that provides support to victims of identity crime. IDCARE can help you to develop a response plan to take the appropriate steps for repairing damage to your reputation, credit history and identity. Visit the IDCARE website at www.idcare.org or call 1300 432 273.

Apply for a **Commonwealth Victims' Certificate**—a certificate helps support your claim that you've been the victim of identity crime and can be used to help re-establish your credentials with government or financial institutions. Visit the Attorney-General's Department at www.ag.gov.au (or call 02 6141 6666) to learn more about protecting and recovering your identity.

Contact a counselling or support service

If you or someone you know has been scammed and may be suffering from emotional stress or depression, please talk to your GP, local health professional or someone you trust. You may also consider contacting counselling or support services, such as:

Lifeline—when you need support in a crisis, contact Lifeline on 13 1114 (24/7) or visit www.lifeline.org.au

Beyondblue—for information about depression or anxiety, contact beyondblue on 1300 224 636 or visit www.beyondblue.org.au

Kids helpline—telephone and online counselling and support service for young people aged between five and 25 years. Contact Kids helpline on 1800 551 800 or visit www.kidshelpline.com.au

Financial Counselling Australia—if you are in financial distress call 1800 007 007 to talk to a free financial counsellor or visit www.financialcounsellingaustralia.org.au.

Where to report a scam

You can help others by reporting a scam to the appropriate authorities. Your information will help these organisations build a better picture of the latest scams and warn other people about what to look our for.

The following organisations take reports about particular types of scams.

Scamwatch

Report scams to the ACCC via Scamwatch—visit www.scamwatch.gov.au

Stay one step ahead of scammers

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

Follow Scamwatch on Twitter at @scamwatch_gov or http://twitter.com/Scamwatch_gov

If you encounter a scam on a website or social media platform, report it to the site so it can be investigated and removed. If the scammers are impersonating a legitimate organisation like a government department or bank, let them know so they can warn others.

Other agencies

You should also consider reporting your scam to other agencies that specifically deal with certain types of scam.

Type of scam	Agency
Cybercrime	Australian Cybercrime Online Reporting Network (ACORN)—visit www.acorn.gov.au
Financial and investment scams	Financial and investment scams Australian Securities and Investments Commission (ASIC)—visit www.moneysmart.gov.au or call the ASIC infoline on 1300 300 630
Fraud and theft	Your local police—call 13 1444
Spam emails and SMS	Australian Communications and Media Authority (ACMA)—visit www.acma.gov.au or call the ACMA Customer Service Centre on 1300 850 115
Tax related scams	Australian Taxation Office (ATO)—to report a tax scam or verify whether a person contacting you from the ATO is legitimate: • call 1800 008 540 or forward your email tax scam to ReportEmailFraud@ato.gov.au
Banking	Your bank or financial institution

Contact your local consumer protection agency

While the ACCC is the national agency dealing with general consumer protection matters, state and territory agencies may also be able to assist you.

Australian Capital Territory Office of Regulatory Services	www.accesscanberra.act.gov.au 13 2281
Consumer Affairs Victoria	www.consumer.vic.gov.au 1300 558 181
New South Wales Fair Trading	www.fairtrading.nsw.gov.au 13 3220
Northern Territory Consumer Affairs	www.consumeraffairs.nt.gov.au 1800 019 319
Queensland Office of Fair Trading	www.fairtrading.qld.gov.au 13 7468
South Australia Consumer and Business Services	www.cbs.sa.gov.au/ 13 1882
Tasmania Consumer, Building and Occupational Services	www.cbos.tas.gov.au/ 1300 654 499
Western Australia Department of Mines, Industry Regulation and Safety	www.consumerprotection.wa.gov.au/ 1300 304 054

More information

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

- Stay Smart Online Service—www.staysmartonline.gov.au
- CyberSmart website—www.cybersmart.gov.au
- Stay Smart Online guides—available at www.staysmartonline.gov.au/get-involved/guides

www.scamwatch.gov.au