ACCC AUSTRALIAN COMPETITION & CONSUMER COMMISSION

The Little Black Book of Scams

A revised version of your guide to spot, avoid and protect yourself against scams.

July 2023

Acknowledgment of country

The ACCC acknowledges the traditional owners and custodians of Country throughout Australia and recognises their continuing connection to the land, sea and community. We pay our respects to them and their cultures; and to their Elders past, present and future.

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

ACCC 07/23_23-43

www.accc.gov.au

Contents

Help is at hand	1
What is a scam	3
Simple steps to spot and avoid scams	4
Text or SMS scams	6
Email scams	9
Phone scams	11
Website scams	13
Social media, online messaging and app-based scams	15
Top scams you should know about	18
Where to report scams	21
More help and support	22

Help is at hand

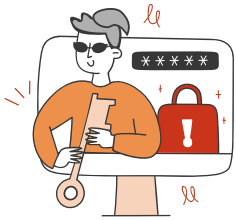
If you're reading this, chances are you, or someone you know has been scammed. Unfortunately, you're not alone. Scams are increasingly sophisticated which means anyone can be a victim of a scam.

If you are a victim of a scam, it's important you act quickly.

- If you've lost money to a scammer, contact your bank or card provider.
- Contact IDCARE on 1800 595 160 or visit www.idcare.org. IDCARE is Australia and New Zealand's national identity and cyber support service. They can help you make a plan (for free) to limit the damage and support you through the process.

Scams succeed because they look like the real thing and catch you off guard when you're not expecting it. Scammers rely on you not spotting warning signs because you're in a hurry, something looks like a great deal you don't want to miss, or because it seems like it's from someone you trust.

Protect yourself from scams by following these 3 simple steps:



STOP

Don't give money or personal information to anyone if unsure.

- Scammers will offer to help you or ask you to verify who you are. They will pretend to be from organisations you know and trust like, Services Australia, police, a bank, government or a fraud service.

THINK

Ask yourself could the message or call be fake?

- Never click a link in a message. Only contact businesses or government using contact information from their official website or through their secure apps. If you're not sure say no, hang up or delete.

PROTECT

Act quickly if something feels wrong.

- Contact your bank if you notice some unusual activity or if a scammer gets your money or information. Seek help from IDCARE and report to ReportCyber and Scamwatch.

What is a scam

A scam is when someone deceives you to steal your money or personal information.

Scams are economic crimes run by criminals who are often very organised and sophisticated.

Scams:

- are run by criminals
- look real
- catch you by surprise
- come with believable stories
- pressure you to take an action

A scam is NOT:

- Computer hacking
- Unfair contract terms
- Harassing marketing approaches

It's important to remember that not all negative experiences are scams. You might have paid for a product that you never received or bought something and found the quality was poor. While this is disappointing, they are not necessarily scams. The Australian Consumer Law offers protections to Australian consumers for these sorts of issues. For more information visit www.accc.gov.au/consumers

Simple steps to spot and avoid scams

Scams can happen to all of us. Scams work because scammers come up with believable stories and tricks to steal your money and get your personal information.

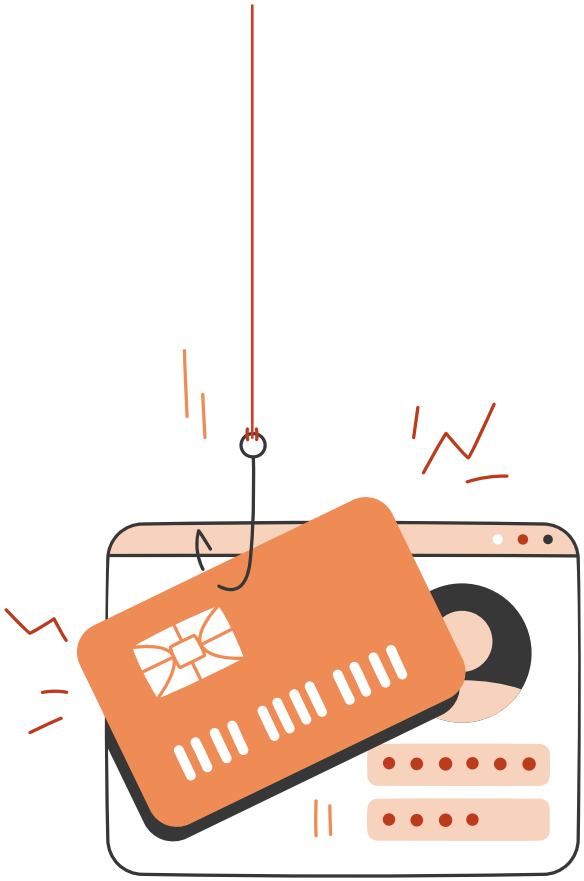
Scammers are getting smarter and taking advantage of new technology, products, services, and major events to convince you that their scams are real.

It can be very hard to spot a scam. Here are some red flags to watch out for. Sometimes scammers use a combination of these tactics.

1. **Opportunities to make or save money:** Scammers will deceive you into believing you're getting an incredible deal or offer. They will put pressure on you to act quickly so you don't miss out. Remember, deals that seem too good to be true, usually are.
2. **Sad stories and cries for help:** Scammers will try and use your good nature against you. They will share stories of heartbreak and tragedy with you and explain why they need your help and your money.
3. **Links and attachments:** Scammers try to catch you off guard and use links to send you to scam websites designed to steal your information and money. Scammers may also ask you to open attachments. These can install viruses that steal your information.
4. **Pressure to act quickly:** Scammers don't want you to take your time and think things through. They want to catch you off guard and pressure you into taking action quickly. This can include making threats that something bad will happen if you don't act fast.
5. **Requests that you pay in unusual or specific ways:** Scammers often ask you to pay using uncommon methods like preloaded debit cards, iTunes cards, or virtual currency like Bitcoin. Once this money is spent, you can't get it back.

6. **Request to set up new accounts or PayIDs:** Scammers may ask you to set up a new bank account or PayID in order to pay them (or be paid by them). They may pretend to be your bank and tell you to transfer your money into new accounts to keep it safe.

If scammers have succeeded in taking your money, they will try to get more money from you. Unfortunately, one in three scam victims have been scammed more than once. If you've lost money to a scam be on the lookout for scammers offering to help you get your money back. This is another kind of follow-up scam.



Text or SMS scams

Scammers send messages pretending to be from the government, law enforcement, trusted businesses, or even your own family or friends.

These messages will sound urgent and try to get you to act quickly. They will often have a link which will take you to a scam website. Scammers can steal any personal information entered on these scam websites and use it to take your money or commit fraud in your name.

To make these messages seem real, scammers copy or mask the phone number and caller ID of businesses or people you know.

Scam messages can even appear in the same message chain as real messages from the organisation, making them even harder to spot.

Signs a message might be a scam

The message:

- Asks you to take immediate action, make a payment, or transfer money.

- Asks you to click on a link or call a number provided in the message.

- Asks you to log on to an online account with your username and password or to provide other personal information.

- Is from a family member or friend saying their contact details have changed.

- Threatens to stop a service or charge you if you don't act.

- Suggests you or your accounts have been hacked or involved in fraud.

- Suggests that there is a problem with your payment or your package delivery.

Steps to protect yourself from messaging scams

1. If someone you know sends a message to say they have a new phone number:
   a. try to call them on the existing number you have for them, and
   b. message them on the new number with a question only they would know the answer to, to check they are who they say they are.

2. Never click on links in messages.

3. If a message links to a website, don't click the link. Instead, search for the website yourself online, or use the official app.

4. Don't respond to a text message using the phone number provided.

5. Call the organisation or person back on a phone number you have found yourself.

Email scams

Scammers send emails pretending to be from the government, law enforcement and businesses. They make it sound urgent to get you to act quickly.

Scammers use the same logo and a similar email address as the real organisation. Scammers can also copy or mask the email address of an organisation or business to make the scam email look more real.

Signs an email might be a scam

The email:

- Requests a payment but the account details are new or have changed since the last payment you made.

- Asks you to log on to an online account with your username and password or to provide other personal information.

- Was unexpected and includes an attachment with an invitation to open it.

- Asks you to confirm your banking details to receive a refund or money you are not expecting.

- Claims to have information about you or images of you and threatens to release them.

- Offers to help you recover money or get compensation for a data breach or identity theft.

Steps you can take to protect yourself from email scams

1. Check that the email is real by either:
   a. contacting the person or organisation directly using contact details you've found yourself such as from the organisation's website or,
   b. accessing an organisation via their official app (never via a link).

2. Immediately cut contact with anyone who tries to threaten or intimidate you.

3. Never give personal details or pay anyone offering you:
   a. compensation or help to recover from a previous scam or data breach or,
   b. winnings, prizes or an inheritance.

4. Use multi-factor authentication when you can. This provides an extra layer of protection and means a scammer has to know your email password and a pin number sent to your phone to gain access to your email account.

Phone scams

Scammers call, claiming to be from well-known organisations. This includes government organisations, law enforcement, investment and law firms, banks, and telecommunication providers.

They make it sound urgent to get you to act quickly. They may try to convince you to give them your personal or bank account details, or access to your computer.

The caller may already have some details about you, such as your name or address, making the call seem real.

Signs a phone call might be a scam

The caller:

- Asks for payment or asks you to move money to a new account.

- Asks you for your password, pin, one-time code, or some other security information.

- Asks you for your financial details, such as credit card or banking details.

- Asks you to complete an action on your mobile phone or computer such as installing software or access a secure account.

- Claims to be from law enforcement and threatens you with immediate arrest or deportation.

- Says your bank or other online accounts have been hacked or involved in fraud.

Steps you can take to protect yourself from phone scams

1. Check that the call is real by either:
   a. contacting the person or organisation directly using contact details you've found yourself such as from the organisation's website or,
   b. accessing an organisation via their official app (never via a link).

2. If you are not sure who a caller is or if they threaten or intimidate you, hang up.

3. Never install software that allows someone access to your computer or device.

4. You can ignore calls from numbers you don't know or let calls go to voicemail.

Good to know!

You can still receive scam calls even if you have a private number or are on the Do Not Call register.

Website scams

Scammers can pretend to be anyone online, including the government, a real business, celebrities or your friends or family.

They can create fake websites to look like well-known brands. They may impersonate famous people and make it look like they are approving goods or services. These websites can contain fake reviews to make you trust them.

You might see fake advertising banners or pop-up windows that contain fake warnings or error messages when online.

Signs a website might be a scam

The website:

- Offers items for sale at significantly lower prices than usual or compared to other sites.

- Tells you about a way to make quick, easy money with little risk or effort.

- Contains an urgent warning or error message asking you to click a link.

- Asks for payment in unusual or specific ways such as gift cards or cryptocurrency such as Bitcoin.

- Only includes positive reviews.

Steps you can take to avoid website scams

1. Compare prices. If an offer appears too good to be true, it probably is.

2. Research the organisation or person you are dealing with before giving your money or personal information.

3. Don't rely on reviews written on the website itself. Search the website or business name and the word 'scam' or 'reviews'.

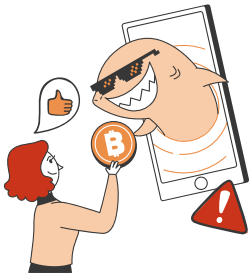
4. If a warning or error message pops up on your screen don't click on it, instead go to the application it refers to directly to check if it is real.

5. Keep the device you use for online shopping up to date by enabling 'automatic updates' for your operating system and apps.

Good to know!

Practical ways to protect yourself online are available on www.cyber.gov.au

Social media, online messaging and app-based scams



If someone you don't know contacts you on social media, a messaging platform like WhatsApp or WeChat, or via an app, it could be a scam. Scammers pretending to be someone else will often contact you out of the blue. They may even use the same logo of the real organisation or photo of the person they are pretending to be to make the scam harder to spot.

Scammers on social media will set up fake profiles and pretend to be from the government, a real business, employer, investment firm, or even a friend, family member or romantic interest.

They may impersonate famous people and make it look like they are promoting goods or services.

Scammers can also learn a lot about you from details you share on your social media accounts and use this information to guess your account passwords or target you with other scams.

Signs of a social media or app scam

The social media profile or app:

- Tells you about a way to make quick, easy money with little risk or effort.

- Invites you to enter a competition or limited time offer.

- Requests to move a conversation from an app such as a dating app to private chat or email.

- Suggests a famous person endorses or supports a product or service.

- Says someone will buy something you are selling without seeing it first and at a high price.

- Threatens to share a private image of you unless you pay them money.

- Contacts you out of the blue offering you a job.

Steps you can take to avoid social media and app-based scams

1. Check if the profile might be fake. Is the account active? How many friends/followers do they have and how much do they post online?

2. Search the name of the profile online together with the word 'scam.'

3. Never take a job you were offered without an interview, or discussion about your experience, suitability, and references. Research the recruiter and the business or individual offering the position. Contact the recruitment agency via phone numbers sourced from an independent internet search. Don't pay money up front just to secure a job.

4. Only take investment advice from someone with an Australian Financial Services license and check that a company or website is not named on the International Organization of Securities Commission's (IOSCO) investor alerts portal.

5. Never give money to a person you have only met online. Scammers often say they live overseas and can't meet you in person.

6. Never send intimate pictures of yourself to someone you have only met online.

Good to know!

Information on how to stay safe on different social media platforms can be found on www.esafety.gov.au

For more information about scams including other ways that scammers might contact you, such as in-person and by mail, visit Scamwatch.

Top scams you should know about

Here are some of the most common scam types for you to be aware of. You can find more information on each of these types of scams, including warning signs and steps to protect yourself, on the Scamwatch website.

Impersonation scams

Scammers deceive you into thinking they are from trusted organisations such as the police, government, banks, and well-known businesses. They can even pretend to be your friend or family member. Scammers fish for information about you by sending phishing emails or messages. These are designed to steal your information. They try and convince you to give them your personal information by pretending they are from an official organisation or someone you know and trust.

Scammers use technology to make their calls or messages appear to come from a legitimate phone number. They can make text messages appear in the same conversation thread as genuine messages from an organisation.

Investment scams

Scammers use convincing marketing and new technology to make their investment sound too good to miss. They promise you big payouts with little or no risk. They often use pressure tactics to get you to act fast, so they can steal your money.

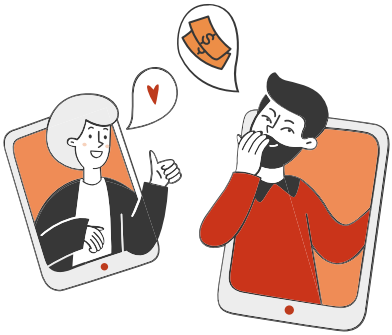
Jobs and employment scams

Scammers offer jobs that pay well with little effort. They pretend to be hiring on behalf of high-profile companies and online shopping platforms. Sometimes, the job they list doesn't even exist. Scammers also impersonate well-known recruitment agencies. Their goal is to steal your money and personal information. The may ask you to pay money up front to be able to work for them.

Products and services scams

Scammers pose as buyers or sellers to steal your money. They set up fake websites or profiles on legitimate retailer sites offering products or services at prices that are too good to be true. They post fake ads and fake reviews. They may use stolen logos, a .com.au domain name and stolen Australian Business Number (ABN). These scams are hard to spot.

Scammers also pose as businesses that you know and trust to send you fake bills. They can even change details on legitimate invoices so that customers end up paying the scammer instead of you.



Romance scams

Scammers use the promise of love, dating, or friendship to get your money. They go to great lengths to convince you the relationship is real and manipulate you to give them money.

Scammers find you on social media, dating or gaming apps and websites. They might also text or email you. They hide behind fake profiles and identities, sometimes of famous people. Once you trust them, they will have an 'emergency' and ask for your help. This will often be requests for money or other products.

Threats and extortion scams

Scammers pretend to be from a trusted organisation and claim you need to pay money or something bad will happen. They may threaten you with arrest, deportation, or even physical harm, if you don't agree to pay them immediately.

They can also blackmail you by threatening to share naked pictures or videos you have sent them unless you send them money.

Unexpected money scams

Scammers try to convince you that you are owed or entitled to, money or winnings that you did not expect to receive.

The scammer asks you to pay a fee or to give your banking or identity details before you can collect the money or winnings. Unfortunately, there is no free money.

Where to report scams

We're working to make Australia a harder target for scammers by raising awareness about how to recognise, avoid, and report scams. We share information from scam reports and work with government, law enforcement, and the private sector to disrupt and prevent scams.

Every report counts, so report your scam experience to Scamwatch via the report form on the Scamwatch website www.scamwatch.gov.au

Remember, if you are a victim of a scam, it's important you act quickly.

- If you've lost money to a scammer, contact your bank or card provider.
- Contact IDCARE on 1800 595 160 or visit www.idcare.org. IDCARE is Australia and New Zealand's national identity and cyber support service. They can help you make a plan (for free) to limit the damage and support you through the process.

More help and support

Being a scam victim can feel overwhelming. It's important to remember that it can happen to anyone, and support is available. If you or someone you know has been scammed, talk to someone about it. You can seek support from family, friends, your GP or one of the following support services.

Lifeline: 13 11 14
or online crisis support chat (24 hours a day, 7 days a week)

Beyond Blue: 1300 22 4636
or online chat (24 hours a day, 7 days a week)

Kids Helpline: 1800 55 1800
(24 hours a day, 7 days a week)

The financial impacts of scams can be devastating and life changing. If you are experiencing financial hardship you can speak with a financial counsellor through the National Debt Helpline:
1800 007 007 from 9:30am – 4:30pm Monday to Friday
or access Live Chat from 9:00am – 8:00pm Monday to Friday


ACCC
AUSTRALIAN COMPETITION
& CONSUMER COMMISSION