Fraud, cybercrime and scams

Information for people affected by scams

Government of South Australia
Victims of Crime SA

Need more information?

Visit our website to find more about:

- what to expect after a crime
- what compensation you might be entitled to
- where you can go for help

Victims of Crime SA acknowledges and respects Aboriginal peoples as the state's First Peoples and nations and recognises Aboriginal peoples as Traditional Owners and occupants of lands and waters in South Australia.

Introduction

This is a guide for people who have been affected by cybercime or fraud. You are a victim of crime and deserve respect and support as you rebuild your life.

Even the most careful people can become victims of fraud. Scams and cybercrime can have lasting impacts that can leave victims feeling emotionally violated as well as financially crippled.

This booklet has information about fraud and scams, things to look out for and what to do if you think you've been caught up in one.

Contents

What is fraud and cybercrime?

Fraud is a crime where somebody deliberately deceives or tricks another person for financial gain or some other benefit or advantage.

Some common words used to describe fraud are:

Fraud also includes cybercrime. It can be cyber enabled or cyber dependent crime and can include:

- hacking
- online scams and fraud
- identity theft
- attacks on computer systems
- illegal or prohibited online content.

With more people using the internet to conduct their business every day, online scams have become more common and incredibly sophisticated.

Types of scams

- Romance or relationship scams
- Advance fee fraud (e.g. up-front payment or inheritance scam)
- Lottery, sweepstakes and competition scams
- Computer hacking
- Online shopping, classifieds and auction scams
- Banking, credit card and online account scams
- Business Email Compromises (email intercept)
- Job and employment scams
- Investment scams (e.g. golden opportunity and gambling scams)
- Charity/assistance and medical scams

This is not an exhaustive list of scams. New types of scams appear all the time.

Scamwatch is run by the Australian Consumer and Competition Commission (ACCC). It provides information about how to recognise, avoid and report scams.

Visit www.scamwatch.gov.au to learn more.

What are the warning signs?

Have any of the following scenarios happened to you?

- Someone you are 'dating' online says they are trying to visit or move to Australia, but something happens to stop them, or they need money.
- You are dating a soldier who needs money for food, equipment, medical fees or to purchase leave.
- You are asked to receive money into your account, then forward this money on, keeping a small handling/admin fee for yourself. This is known as a work from home or employment scam.
- You have received cold calls, unsolicited email or texts, or have been contacted via social media.
- You have been asked to confirm, update or provide your account or personal information.
- You have been contacted by a number of different 'officials' who want money. You have been promised a large windfall or inheritance but have to make payments to get it released.
- You win an overseas lottery or competition despite never having entered.
- You have been pressured to buy stocks or shares often via a cold call.
- You have been contacted or threatened with arrest or summons for unpaid tax bills or fines with the promise of refunds.

- You are communicating with a government official, doctor, lawyer or ‘police officer’ that uses Gmail, Hotmail or any other free web-based email service.
- You are asked to pay fees or fines via international fund transfer, cards such as iTunes or Google Play cards, or by purchasing crypto currency (e.g. bitcoin).
- You are selling an item online and someone responds with a generous offer - then has ‘accidentally’ overpaid or requires up front freight costs.
- You receive a request to allow ‘remote access’ to your computer.

Every year hundreds of people are victims of frauds and scams. If you are concerned that you may be a victim speak to police or a trusted person

Scammer tactics

Scammers use a lot of sophisticated and effective psychological tricks to target, influence and manipulate their prospective victims.

They often change their tactics depending on the situation.

Emotional manipulation

Scammers will play on your emotions. They may use threats, encourage certain behaviour, create emotional fear, make you feel despair or guilt, or just rely on you feeling love for them.

Some people have said they felt as though they were hypnotised or groomed.

Using photos and video

Scammers often produce photographs or have a face-to-face conversation via video chat or social media to try and establish or reinforce their authenticity.

Remember, people are not always who they claim to be and can be located anywhere in the world.

Scammers can use photographs or video footage of others from the internet to deceive their targets or use others to communicate on their behalf.

Pressure tactics

Scammers will aim to isolate you and ask you to do things within a very short timeframe. This is so you send money before having time to step back and look at the bigger picture, do any research or consult with trusted family, friends or professionals.

They may ask you to complete a document using your personal information (e.g. passports). This can be used to steal and use your identity.

Exploiting vulnerabilities

Scammers will often exploit a person's vulnerabilities. Many scammers target people looking for companionship via internet dating sites. They quickly build a relationship with their victim.

They may ask you to send explicit photographs of yourself which they can then use to blackmail or extort you into sending money to stop their release.

Moving conversations to different platforms

After speaking with you for a while, scammers will often try to move your conversations off the original platform and onto different encrypted apps. For example, moving conversations off of Facebook and onto WhatsApp.

Moving to an encrypted app makes the conversations and the scammer more difficult to track down.

Romance or relationship scams

One of the most common scams is a romance or relationship scam.

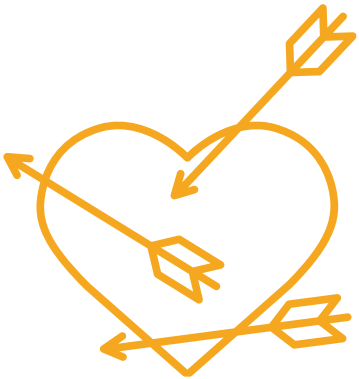
Scammers can target people through legitimate dating sites and apps, as well as through social media.

Often, scammers will find people who might not be actively looking for companionship, but meet certain criteria like age or marital status (divorced or widowed).

They will establish a relationship with you and gain your trust. They may share personal information, express strong feelings for you and even send you gifts.

This is known as 'cyber grooming' and may go on for many months before they ask for money.

Eventually they might talk about visiting you and tell you they have booked flights. However, they often say they have missed the flight then give any number of reasons.



Some of the fake excuses people have been given include:

- a car accident on the way to the hospital
- corrupt immigration officials demanding bribe money to allow them passage
- corrupt customs officers demanding bribes to turn a blind eye to gold/diamonds/cash that is being smuggled out of the country
- a sick relative was rushed to hospital or in need of lifesaving medical care
- a child or family member has suddenly gone missing
- someone in their life is threatening them to stop them leaving
- they are in custody or detention, or are facing deportation
- they have been kidnapped.

This will then lead to more demands for money to help with:

- replacement tickets
- cancellation fees or visas
- medical and rehabilitation expenses
- bribe money for public officials
- legal fees
- food/living and education expenses
- business start-up money.

Scammers will try to use any excuse that will tug at your emotions or conscience.

In some cases, the scammer will pretend to be a soldier and explain that they:

> can't get enough money to buy equipment/ food or to purchase extra leave

> have been wounded, but the US/AUS government won't cover their hospital expenses.

The love interest may also ask you to:

> transfer a large sum of money for them.

> help transport packages between countries. Authorities have detected drugs and other illegal items hidden in luggage or packaging.

Receiving or transferring money or property could amount to money laundering which is a serious criminal offence, and you could be prosecuted.

Who do scammers target?

Many people think that victims of scams are greedy, risk-taking individuals looking to make money, or they are naïve or uneducated.

This is not true.

People of all ages, backgrounds and social standing can be victims of scams.

Some scammers target people who are experiencing financial difficulties or personal issues because they may be particularly receptive to a proposal that promises profits.

Often fraudulent cold-callers will target the elderly because they are more likely to:

> have money, property, savings and investments
> be home to receive phone solicitations
> remain on the phone longer to hear a fraudulent sales pitch.

Scammers can target people who:

> lack experience in recognising fraudulent pitches
> have a desire to increase their standard of living quickly
> lack information about financial investments
> are compassionate or trusting
> are lonely or isolated.

Protecting yourself

Do not divulge personal details or passwords.

Don't accept friend requests from people you either don't know or don't have mutual friends with.

Increase privacy settings on all your professional and personal social media accounts.

Consider changing your profile pictures and username.

Limit the personal information that you post online, including photos or documents.

Remember - if a deal looks too good to be true, it probably is.

You may want to delete your email address and create a new one.

Keep your computer's security protection up-to-date. Seek professional advice or ask for help from family members.

Never click on images or links in emails or text messages. Go to the website's page using a search engine (eg. Google search).

Always verify unpaid bills, fines or offers of returns with the relevant government agency (e.g. Australian Taxation Office).

Never send money via international funds transfer, or store cards (e.g. iTunes and google play cards) or crypto currency.

Research and check everything. Do not rely on the information provided. Ask police or a trusted person who can help you with this.

Repeat approaches

Once you have been scammed there is a real threat of it happening again.

It may not be the original scammer trying to get more money though – your details could have been sold on to a new group of scammers.

Keep an eye out for these warning signs:

> The scammer will aggressively deny the scam, then employ pressure tactics to get you to continue sending money.

> The scammer comes clean to you. They may claim that while targeting you, they have genuinely fallen in love and will help you recover some of your money.

> Someone says they can get your money back (e.g. a solicitor or law firm, law enforcement agency or other agency). They will ask you for fees to recover your losses.

These are all methods to try and get you to part with your money. A lot of these tactics will be aimed at playing on your emotions and pressuring you.

What do I do now?

If you believe you have been the victim of a scam, you should report it to the police – even if you feel embarrassed.

Reporting scams to police

When speaking to police try to be as prepared and organised as you can. Take any evidence or information you think will help to support what you are saying.

By contacting police you can prevent other people from becoming victims.

More information about scams is on the SAPOL website.

Web: www.police.sa.gov.au/scams
Phone: 131 444

You can also visit your local police station. See www.police.sa.gov.au to find your closest station.

Call investigators

Sometimes the police become aware of scams and will get in touch with affected people. If you have received a letter from police, use the contact details contained within the letter to discuss the matter with police, as well as a trusted person.

Reporting cybercrime

You can report a cybercrime or online scam via the Australian Cyber Security Centre's ReportCyber portal.

This is a national online reporting system where you can securely report instances of cybercrime.

Your report will then be referred to the appropriate police jurisdiction for assessment.

Web: www.cyber.gov.au/acsc/report

Dealing with the scammer

If you have reported the scam to police, make sure you:

- stop sending money immediately.
- cease all communication.
- contact your financial institution, tell them about the situation and ask for their help in changing your account and card details.
- consider changing your phone numbers or SIM card, email and social media accounts, usernames and passwords.
- report your matter online to ReportCyber - any documented evidence helps.
- be aware that your personal details may have been passed to other scammers who will try to get money from you and continue the cycle.

Do not engage with the scammers for any reason – not even to tell them you know what they are up to. It will simply give them the opportunity to pressure and persuade you that you are wrong.

In some cases, you may have to accept that the money you have sent is gone.

Impact of fraud

Cybercrimes, frauds and scams can have a lasting impact on victims.

These crimes are often complex, financially crippling and can leave people feeling emotionally violated.

Being scammed can be a significant breach of trust.

Some people have had to return to work after retirement as they have been scammed of their lifesavings or superannuation.

Some people describe experiencing a range of emotions like victims of robbery or a house break-in. Others report suffering trauma similar to that of violent crime.

How you might feel

Those affected by fraud commonly experience:

- denial
- financial hardship for individuals and their families
- stress and anxiety
- confusion
- panic
- loneliness and isolation
- feeling powerless and manipulated
- feelings of embarrassment and foolishness
- feeling like their personal space has been invaded or violated
- loss of self-esteem
- a change in social status and/or social isolation
- relationship difficulties
- self-blame
- feeling judged by others.

People affected by fraud and cybercrime can experience a combination of these and other reactions.

You might feel like this for a few days, weeks, months or longer.

The reactions will vary from person to person and may change over time. For example, there will be days you feel you are coping well and other days when you may feel overwhelmed.

Feeling judged and embarrassed

It is not for anyone else to judge how much a scam has affected you. No one knows how they would have reacted under the same circumstances.

Avoid blaming yourself and put the blame where it belongs - on the criminal who scammed you.

> Remember that scammers are very clever and manipulative. Don't let others make you feel guilty or foolish.

Do not be afraid to seek help when you need it whether it be from family, friends and/or professional counsellors.

Remember it will take time to recover but if you are concerned or overwhelmed by the way you are feeling you should consult your doctor or a counsellor.

Where can I get help?

South Australia Police

000	Police, Fire, Ambulance in an emergency
131 444	Police Assistance Line for non-urgent police assistance
1800 333 000	Crime Stoppers report crime anonymously

Web: www.police.sa.gov.au

Australian Cyber Security Centre (ACSC)

The Australian Cyber Security Centre provides advice and information about how to protect yourself, your family and your business online. Their **ReportCyber** portal is a national online reporting system that allows the public to securely report instances of cybercrime including:

- hacking
- online scams
- online fraud
- identity theft
- attacks on computer systems.

Web: www.cyber.gov.au/acsc/report

Scamwatch

Scamwatch is run by the Australian Competition and Consumer Commission (ACCC). It provides information to consumers and small businesses about how to recognise, avoid and report scams. Visit their website for more information on how scams work, how to protect yourself and what to do if you've been scammed

Web: www.scamwatch.gov.au

IDCARE

IDCARE is Australia and New Zealand's national identity and cyber support service. IDCARE have helped thousands of individuals and organisations reduce the harm they experience from the compromise and misuse of their identity information by providing effective response and mitigation.

IDCARE can help with:

- a tailored Response Plan to your circumstances
- a dedicated Case Manager who can work with you to address your needs
- a premium support service if your service provider is an IDCARE member organisation where IDCARE can carry some of your load.
- when an issue arises outside of their expertise, they will do their best to refer you to an organisation who can help.

Phone: 1800 595 160 or (08) 7078 7741
Web: www.idcare.org

Victims of Crime SA

Victims of Crime SA is led by the Commissioner for Victims' Rights and supports South Australian victims of crime. The office can:

- provide information, advice and support
- help to deal with the physical, emotional and financial impact of crime
- help victims in their dealing with prosecution authorities and government agencies.

The Commissioner is an independent statutory officer appointed to help victims of crime, advocate on their behalf and ensure their rights are upheld. The Commissioner also monitors and reviews laws and court practices on victims.

Phone: 7322 7007
Email: victimsofcrime@sa.gov.au
Web: www.voc.sa.gov.au

rebuild. Counselling for Victims of Crime

rebuild provides trauma-based counselling and peer support to adult and child victims of crime as they move through the criminal justice process. The service is for:

- anyone directly harmed by a crime
- anyone harmed as a result of witnessing a crime
- parents or caregivers who have been harmed as a result of a crime against their child
- relatives of a person who has died or suffered harm as a result of the crime.

This is a confidential and free service available state-wide. Counselling and support is available face to face, by telephone or online video appointment.

Phone counselling via TTY and TIS is also available.

Hours: 9.00am to 5.00pm | Monday to Friday
Phone: 1800 310 310 during business hours to make an appointment or to leave a voicemail
Email: rebuild@rasa.org.au
Web: www.rasa.org.au/rebuild

General Practitioner / Family Doctor

Ask your doctor for a 30 minute consultation and a Mental Health Care Plan.

General practitioners can refer for up to 12 individual consultations and 12 group sessions with a psychologist, social worker or occupational therapist - all with a MEDICARE rebate - Health Care Card holders will have no gap fees but some providers do charge others a gap. Enquire before making a booking.

Lifeline

Lifeline provides all Australians experiencing a personal crisis with access to online, phone and face-to-face crisis support and suicide prevention services.

Phone: 13 11 14
Web: www.lifeline.org.au

eSafety Commissioner

The Australian eSafety Commissioner works to keep all Australians safe online. They provide a range of guidance on specific online issues including:

- online scams
- cyberbullying
- adult cyber abuse
- image-based abuse
- technology-related concerns for people at risk of family or domestic violence.

They also run the Be Connected initiative, which focuses on increasing confidence, skills and online safety for older Australians.

Web: www.esafety.gov.au

Government of South Australia
Victims of Crime SA

November 2022