

Be safe Be alert online

Online safety and security quick reference guide



Australian Government agencies are here to support you

eSafety Commissioner



About the agency

The eSafety Commissioner (eSafety) is Australia's national independent regulator for online safety, leading and coordinating online safety efforts across government, industry and the community.

eSafety investigates complaints about cyberbullying of children, image-based abuse and illegal online content, to help get the harmful content taken down from the internet.

eSafety also provides online safety information and guidance through our website and offers educational resources and training to help parents and schools.

Safer Internet Day

In February each year, eSafety leads the Safer Internet Day campaign, to raise awareness about online safety and to promote the responsible and positive use of digital technology.



Top tips for staying safe online

- ★ **Be an upstander** — if you see abuse online, report and delete it.
- ★ **Protect your personal information** — use a different password for each account and turn on privacy settings on devices, apps and social accounts.
- ★ **Tame the tech** — explore how to set access and parental controls on home wifi networks, gaming consoles, mobile devices and smart TVs.
- ★ **Be conscious of your online profile** — don't post anything that could put you in danger, affect your reputation or be used against you.
- ★ **Help others to be safe online** — especially children, family and friends who aren't tech-savvy or safety-conscious.



Get in touch



esafety.gov.au/subscribe



[@eSafetyoffice](https://twitter.com/eSafetyoffice)



[esafetyoffice](https://www.linkedin.com/company/esafetyoffice)



[eSafetyOffice](https://www.facebook.com/eSafetyOffice)

eSafety Commissioner

General online safety advice

As the Federal Government's online safety support and coordination agency, eSafety provides evidence-based and audience-specific support, research and resources to help inform the Australian community about online safety. We focus on young people, parents, educators, women, older Australians and other at-risk communities.

Support for community organisations

eSafety offers a range of resources to help community groups, clubs and sporting organisations improve their online safety knowledge and skills to inform their policies and practices. Organisations can book a free eSafety webinar or presentation that covers a range of online safety related topics including the risks and how to manage and mitigate negative online experiences.

eSafety Parents

eSafety provides practical advice and resources for parents to help their children have safer experiences online. Our eSafety Guide offers parents and carers the latest information on videoconferencing services, games, apps and social media.

eSafety Women

Technology-facilitated abuse is an emerging trend and can take many forms such as:

- abusive messages or calls
- online account take overs
- harassment from fake social media accounts
- being tracked through a phone or device.

eSafety's guidance helps women (and frontline support workers) learn to recognise these forms of abuse and what protective steps to take if it occurs.

Keeping young people safe

eSafety provides best-practice online safety education resources and training for early childhood educators, teachers, schools, universities and communities. eSafety's guidance aims to empower, build resilience and effect positive change by promoting the development of safe and appropriate online behaviours.

Helping older Australians be safer online

Since 2017, eSafety has partnered with the Department of Social Services and Good Things Foundation to help improve digital literacy among older Australians. Under the Be Connected program, eSafety has developed an e-learning portal, interactive content, webinar-based training and an intergenerational mentoring program.

Protection from online harms

eSafety protects Australians from online harms through its reporting, investigations and notification schemes. Members of the public can make a report to eSafety and get help having content taken down.

Cyberbullying

We assist and support young people under 18 who are being bullied online. We can help to remove serious cyberbullying content that is threatening, intimidating, harassing or humiliating.

Image-based abuse

If an intimate image has been shared without consent, or threatened to be shared, Australians can report it to eSafety. We help with getting intimate images or videos removed through a range of enforceable actions and offer further advice and support to victims.

Cyber Report

eSafety investigates complaints from Australian residents and law enforcement agencies about illegal and seriously harmful online content and has regulatory powers to enforce removal. If you encounter child sexual abuse material online report it to eSafety.

Australian Cyber Security Centre

i

About the agency

The Australian Cyber Security Centre (ACSC) is based within the Australian Signals Directorate (ASD). The centre provides advice, assistance and operational responses to governments, businesses and individuals to prevent, detect and remediate cyber security threats to Australia.

The ACSC's cyber security mission is supported by ASD's wider organisation, whose role is to produce foreign signals intelligence. The ACSC leads the Australian Government's efforts to improve cyber security. We also perform activities to prevent and disrupt offshore cyber-enabled crime.

Our role is to help make Australia the safest place to connect online.

Stay Smart Online Week

Each year in October the ACSC runs Stay Smart Online Week, to raise awareness about the ways people can protect themselves online.



Australian Government
Australian Signals Directorate

ACSC

Australian
Cyber Security
Centre



Top tips to protect your security online

- ★ **Secure important accounts** such as email, banking and social media by turning on two-factor authentication.
- ★ **Use a password manager** to generate and store unique credentials where possible. Use unique passphrases otherwise.
- ★ **Watch out for scams.** Never provide your personal information or passphrases in response to unsolicited messages. Always use the official app or website.
- ★ **Always use a biometric, PIN or passphrase** to lock your devices – especially the portable ones.
- ★ **Apply all software updates** and turn on automatic updates where possible.
- ★ **Don't use unsupported operating systems** like Windows 7, Android 7 and iOS 12 (iPhone 6) for important tasks.
- ★ **Backup important data** using external USB hard drives. Store these separately to the device.



Get in touch



cyber.gov.au/report



@CyberGovAu



Stay Smart Online

ACSC Alert Service
cyber.gov.au/alert-service

cyber.gov.au

Australian Cyber Security Centre

Protecting your business and yourself online

We prevent cyber incidents by working with governments, industry and the community to increase awareness of cyber security and stop threats before they happen.

We educate and inform Australians on current threats and what good cyber security looks like. The ACSC's **Easy Steps Guide** shows how you can better protect yourself from threats and secure your accounts and devices, by stepping through a six-day plan.

Our Small Business Cyber Security Guide is a great place for small businesses to learn how to protect themselves from the most common security incident.

The ACSC Partnership Program

The ACSC Partnership Program enables a wide range of organisations to engage with the ACSC and fellow partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy.



Australian Government
Australian Signals Directorate

ACSC

Australian
Cyber Security
Centre

Stay Smart Online Program

The ACSC's Stay Smart Online program provides topical and timely information on how home internet users and small businesses can protect themselves from cyber security threats such as software vulnerabilities, online scams, malicious activities and risky online behaviours. The program was first established in 2006 and today involves a community of over 95,000 followers, all committed to sharing cyber security information.

Monitoring cyber threats 24 hours a day

The ACSC monitors cyber security threats through advanced cyber threat detection and warning systems. We respond to cyber security threats and incidents as Australia's computer emergency response team. We work with businesses, government and academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats.

Our Joint Cyber Security Centres are hubs for ACSC partners from organisations of all different sizes and sectors to come together across the country and share their knowledge, insights and experience.

Helping to minimise harm during and after a cyber incident

We provide expert guidance to businesses who need help during a cyber incident. We share threat intelligence, incident management and crisis communications advice to assist organisations to minimise harm to their networks, customer information and reputation.

Report Cyber

The ACSC's online reporting tool ReportCyber assists members of the community to report cybercrimes such as hacking, scams, fraud, identity theft, and attacks on computer systems. On average, the ACSC receives one report every 10 minutes. The average amount reported lost is \$5,700 with an average \$829,000 in reported losses to cybercrime every day in Australia—and these are just the cases that get reported.

The reported information is referred to federal, state, or regulatory agencies within the relevant jurisdictions for investigation and in some cases, police action. The data collected from these reports also helps us to track and share trends and patterns in cybercrime as they are reported.

[cyber.gov.au](https://www.cyber.gov.au)

Australian Competition and Consumer Commission (Scamwatch)



About the agency

The Australian Competition and Consumer Commission (ACCC) is responsible for enforcing the Australian Competition and Consumer Act 2010. The ACCC also administers the **Scamwatch** website which provides information to consumers and small businesses about how to recognise, avoid and report scams.

Scams target people of all backgrounds, ages and income levels across Australia. There is no one group of people who are more likely to become a victim of a scam. All of us may be vulnerable to a scam at some time.

Scams Awareness Week

The ACCC coordinates the Scams Awareness Network which collaboratively delivers the annual National Scams Awareness Week campaign. Each year focuses on a unique theme centred around learning how to identify, avoid and report scams.



Top tips to avoid being scammed

- ★ **Scammers often pretend** to be trusted organisations such as the government, banks, energy or telecommunications companies.
- ★ **Beware of requests for your details or money.** Never send money, personal or financial details, or copies of identity documents to anyone you don't know or trust.
- ★ **Never click on hyperlinks or open attachments** in suspicious emails or text messages. Verify the contact using an independent source like an online search.
- ★ **Don't respond to phone calls** about your computer asking for remote access – hang up.
- ★ **Be wary of unusual payment requests** such as preloaded debit or gift cards, up-front wire transfers or virtual currency such as Bitcoin.
- ★ **Verify any changes to bank account details** by directly calling the individual or business you are dealing with using trusted contact details.
- ★ **If an offer seems too good to be true, it probably is.**



Get in touch



scamwatch.gov.au/report-a-scam



@Scamwatch_gov



www.scamwatch.gov.au/subscribe



ACCC AUSTRALIAN
COMPETITION
& CONSUMER
COMMISSION



scamwatch.gov.au

Australian Competition and Consumer Commission (Scamwatch)

Raising awareness about scams

Scamwatch receives well over 100,000 scam reports each year. We aim to reduce the impact of scams by raising awareness and encouraging the public to talk about scams and report them. Through Scamwatch, the ACCC keeps Australians informed with regular warnings and information about common and emerging scams.

Radar alerts

Members of the public can keep up-to-date with the latest scam threats by signing up to receive free Scamwatch radar alert emails.

The little black book of scams

The little black book of scams is a handy tool for consumers and small businesses to learn about common scams, the warning signs and ways to protect yourself. The book is also available online in a number of languages other than English.

Reporting scams to Scamwatch

You can help disrupt scams and warn others by reporting them to Scamwatch.

The ACCC and Scamwatch team greatly appreciate your contribution to the collection of scams-related data. This information is used to keep Australians informed about the latest scams.

We also share information you provide about scammers with law enforcement and other government agencies to combat and disrupt scam activity.

In some instances, when you have agreed, we also share information from reports with private organisations including platform operators and financial institutions as they play an important role in stopping scams and protecting the community.

Many scammers are based overseas and international cooperation by law enforcement is required to investigate and prosecute them. Unfortunately, it is difficult for government agencies to track down and take action against scammers. Government, law enforcement, individuals and businesses all play an important role in helping to protect the community from scams. You can also help by sharing information about scams when connecting with your friends, family and colleagues.

Where to get help

If you have lost money to a scam or given out your personal details to a scammer, it is unlikely you will get your money back.

There are steps you can take straight away to limit the damage and protect yourself from further loss.

If you've sent money or banking details to a scammer, contact your financial institution immediately. They may be able to stop a transaction, or close your account if the scammer has your account details.

If you've given your Tax File Number or superannuation details to a scammer, contact the ATO and your superannuation fund immediately.

If unsure whether you're being scammed, stop sending money. Scammers will keep asking for more money until you stop.

If you suspect you are a victim of identity theft, it's important that you act quickly to reduce your risk of financial loss or other damages. Contact **iDcare** — they can provide specialist support and guidance when faced with an identity related issue.



Office of the Australian Information Commissioner

i

About the agency

The Office of the Australian Information Commissioner (OAIC) is the independent national regulator for privacy and freedom of information.

We work to promote and uphold your privacy rights and increase public trust and confidence in the protection of personal information.

We investigate privacy complaints and data breaches. We also take regulatory action against serious and systemic breaches of privacy and provide advice and guidance for organisations and the community to help them protect and secure personal information.

Privacy Awareness Week

The OAIC leads a Privacy Awareness Week campaign each May to highlight the importance of protecting personal information.



Top tips to protect and secure your personal information online

- ★ **Protect your accounts** with strong and unique passphrases, multi-factor authentication and automatic updates for your devices.
- ★ **Guard against identity theft** and data breaches by shopping through secure sites and watching out for phishing messages that ask you to click a link or provide your personal information.
- ★ **Control your privacy settings** on social media and other digital platforms and be aware of what you share online.
- ★ **Be smart about connected devices**, research privacy and security credentials before you buy, and limit internet access when it's not needed.
- ★ **Take steps to limit location and online activity tracking** through devices, browsers and apps if it's not required for functionality, and clear your cookies and cache regularly.



Get in touch



oaic.gov.au/contact-us



[@OAICgov](https://twitter.com/OAICgov)



Office of the Australian Information Commissioner



[OAICgov](https://www.facebook.com/OAICgov)

OAIC



Australian Government

Office of the Australian Information Commissioner

oaic.gov.au

Office of the Australian Information Commissioner

Protecting your privacy and personal information online

The OAIC protects your privacy rights by investigating and resolving complaints from individuals against organisations covered by the *Privacy Act 1988*. This includes businesses with an annual turnover of more than \$3 million, private health service providers, the consumer credit reporting sector, and Australian Government, ACT and Norfolk Island agencies.

If you are concerned about the way an organisation covered by the *Privacy Act* has managed your personal information, and you're not satisfied with their response to your complaint, you can complain to us.

We can try and reach a resolution by agreement between you and the organisation to solve the issue. We can also investigate the matter and may require them to address the issue. For example, by providing access to your personal information, providing an apology or compensation, changing their privacy practices, or facing further regulatory action.

Online privacy protections

We are working to **enhance online privacy protections** by developing a binding privacy code for online platforms and social media, advising on reforms to Australia's privacy framework, and sharing guidance and resources.

We can take **regulatory action** for breaches of the Privacy Act online, including failure to secure personal information against cyber-attacks.

The OAIC oversees the handling of personal information collected by the **COVIDSafe contact tracing app** and National COVIDSafe Data Store. We can investigate complaints and other privacy issues, audit the system, and refer breaches to the Australian Federal Police for criminal investigation.

We also regulate the privacy aspects of the **My Health Record** system, including handling privacy complaints and receiving any data breach notifications.

We are responsible for enforcing the privacy safeguards under the new **Consumer Data Right** (CDR), which aims to give you greater choice and control over your data. We publish guidance for CDR providers on how to comply with the privacy safeguards, and we can investigate complaints about how your CDR data has been handled.

Investigating data breaches

The OAIC enforces the Notifiable Data Breaches scheme and privacy principles which require organisations and agencies to quickly contain, manage and assess a data breach involving personal information.

They must notify you if your personal information has been lost, or accessed or disclosed without authorisation, and you may suffer serious harm as a result. They must also provide you with advice on how you can minimise the risk of harm.

We can direct organisations to notify you. We also investigate failures to comply with the law.

Privacy advice and guidance

We help organisations and agencies protect your personal information and adopt privacy best practice through our guidance, advice and training resources.

You can find out how to exercise your privacy rights and make a privacy complaint on our website. We've also published advice about your credit report, how to reduce your risk of harm after a data breach, and how to protect your privacy online.

OAIC



Australian Government
Office of the Australian Information Commissioner

oaic.gov.au

Be Safe Be Alert online

Online safety and security quick reference guide

- Reporting of child cyberbullying, image-based abuse and illegal or harmful online content: esafety.gov.au/report
- Digital literacy training and support for older Australians: beconnected.esafety.gov.au
- Reporting of cybercrime or identity theft: cyber.gov.au/report
- Reporting a scam: scamwatch.gov.au/report-a-scam
- Help to protect your personal information online: oaic.gov.au/rebootyourprivacy
- Help with identify theft and related issues: [iDcare.org](https://idcare.org) or call 1800 595 160
- Help with financial and investment scams: ASIC.gov.au
- For Scams and ID theft linked to myGov accounts (Centrelink, Medicare, Child Support):
Call the Services Australia - Scams and Identity Theft Helpdesk on 1800 941 126
or visit servicesaustralia.gov.au/scams
- Report fraud and theft to the Police Assistance Line on 131 444
- Verify or report a scam to the Australian Tax Office: ato.gov.au/scams