Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Protect yourself online

A guide to cyber security for young people

Content Complexity
SIMPLE

cyber.gov.au

For more cyber security advice

For more information on how to improve your cyber security, see our other guides at cyber.gov.au

Personal Cyber Security Series

Security tips for online gaming

Secure your mobile phone

Table of contents

In today's digital age, you need to think about your online security.

The internet provides many ways to learn and chat to friends, but it also exposes you to online threats.

You could have your identity and money stolen, or someone could take advantage of you in other ways.

The steps in this guide can help you navigate the online world with confidence.

Tips for securing accounts and devices

Cybercriminals use many tactics to carry out their attacks. Common devices they target include your smartphone, tablet, computer or gaming console.

Below are things that you should do to reduce the risks.

If you are still unsure or need immediate help, report it or reach out to someone you trust. If something bad has happened, find out how to get help below (page 8).

Create strong passwords or passphrases

A passphrase is even better than a password. It is harder for cybercriminals to guess and easy for you to remember.

A secure passphrase has at least 14 characters using four or more random words. For example, 'purple duck potato boat'.

You should use a different passphrase for each account. Especially if they contain personal information such as your name, address or date of birth. If someone hacks your account, it means that they are less likely to get into your other accounts.

To learn more, visit cyber.gov.au/learn/passphrases

Turn on multi-factor authentication (MFA)

MFA is when you use two or more proofs of identity to log in. For example, using your login details as well as an authentication code.

MFA puts an extra shield around your account. It is one of the best ways to protect yourself from cybercriminals.

If someone guesses or steals your passphrase, they need another step to get into your account.

To learn more, visit cyber.gov.au/learn/mfa

Keep devices and software up to date

Regular updates make your devices more secure. Check automatic updates are on and install updates as soon as you can.

To learn more, visit cyber.gov.au/learn/updates

Back up your data

A backup is a digital copy of your important data such as photos or files.

If you lose your device or it's stolen, you can use a backup to get your data back. You can store backups in the cloud or on an external hard drive.

To learn more, visit cyber.gov.au/learn/backups

Disable geolocation services

Geolocation is when you can track the location of your device. Be careful not to share your location online with strangers or on public sites.

Always check location services for each of your apps under device settings. Most apps don't need to know your location. Think about deleting apps where you can't turn it off.

Disable photo and camera access

Some apps will ask for access to your camera and photos. Always check and adjust this setting for each of your apps. Most apps don't need to access your camera and photos.

You can also choose which photos you want to share instead of sharing them all.

Sharing family devices

If you share devices with your family, make sure they know how to be cyber secure.

Ask them to:

- use strong passphrases
- turn on MFA
- keep devices updated.

Together, you can create a safer digital space for you and your family.

Bring your own device

If you bring your devices to school or other public places, take extra care to:

- lock your device when not in use
- avoid connecting to unknown Wi-Fi networks
- think twice about what you share or access while on your school network.

Remember to follow your school policy on device use and security.

Social media and gaming

Social media and online gaming is a fun way to connect with your friends, relax and build skills. But not everyone online is who they say they are.

Gaming

Be aware of the potential risks of gaming. When playing games online, you might meet people who have bad intentions.

Never share your personal details with someone you don't know. Tell a friend or adult you trust if someone contacts you in a way that is suspicious or makes you uncomfortable.

Be aware of phishing scams in games. Scammers may offer you things that seem too good to be true. For example, free upgrades, in-game currencies, or rare character items. Think before you trade or lend items since you may not get them back.

Only download things from an official game or app store. Avoid visiting suspicious links or downloading unknown files. Don't give out your personal details or money without first checking the source.

Be alert for scams, malware and other vulnerabilities in gaming forums and chat platforms. It is common for cybercriminals to target users with malicious links or attachments. Make sure to look out for anything unusual.

Learn more by going to:

- cyber.gov.au and search 'gaming', 'scams' and 'malware'
- esafety.gov.au/young-people/online-gaming

Social media

If you use social media, you might have 'friends' or 'followers' who you haven't met in real life. You may also follow your favourite celebrities or official fan sites.

Many profiles and websites are safe to follow or use. But it is easy for people to pretend to be someone else online by using fake profile images.

For more safety tips about the latest games, apps and social media, visit esafety.gov.au

Case study

A teenager from WA made an online friend on the social messaging platform Discord. The two friends chatted online and played Minecraft together.

Through Discord, the online friend shared a file and told the teenager to download it. Even though they felt unsure about it, the teenager decided to trust the online friend. When the teenager opened the file, a malicious screen opened and closed.

The online friend then sent back personal information about the teenager to threaten them. This included details such as their device location and email address, which cybercriminals can profit from. This incident could expose the teenager or their family to further attacks and scams.

More tips

Here are some extra tips to keep you secure when chatting and gaming online.

- **Check your privacy settings:**
  Limit who can see your posts and personal details on your social profiles. Never share sensitive details online such as your address, phone number, or date of birth. Sharing photos can even put you at risk, as it may show your school uniform or location metadata. The less you share the better. For more information on how to protect your identity, visit esafety.gov.au
- **Use legitimate software:**
  Always get apps and games from a trusted physical store, online retailer or app store.
- **Avoid saving payment details:**
  If you have your own bank account, avoid saving payment details in your apps and accounts. This includes your credit card or bank details. Some devices have a setting that asks for a password when downloading an app. You can also set the app to prompt for your password after you are inactive.
- **Don't accept friend requests from strangers:**
  Cybercriminals will pretend to be someone your age or even someone from your school. Ignore and report anyone that makes you feel uncomfortable or acts in a suspicious way.
- **Be suspicious of unsolicited messages:**
  This includes a phone call, SMS, instant message, in-game chat or email. Scammers often get you to give them your bank details or open a file. If someone has sent you an unsolicited request, ignore it and report them through Scamwatch at scamwatch.gov.au
- **Check the URL of websites:**
  When you visit any website, make sure the web address (URL) is the real one. Scammers can create fake websites with subtle differences, even one letter. This can be tricky to spot, so check the domain name and spelling is correct.
- **Be careful when shopping online:**
  If you buy something online, the URL should start with 'https' and have the company's name. Don't visit links or use contact details sent to you from someone you don't know. If in doubt, contact the company through their official website.

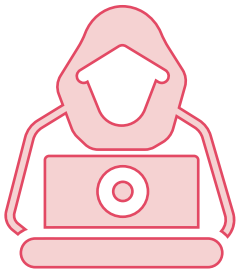
How to get help

Did something bad already happen to you? Find out what to do based on the following scenarios.

Report incidents through ReportCyber at cyber.gov.au/report. ReportCyber also has information on who to contact for help and advice. If you need urgent help, call our 24/7 Hotline: 1300 CYBER1 (1300 292 371).

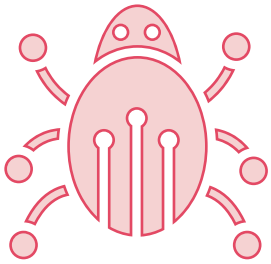
Someone stole your money, data or identity

Change your hacked account passwords straight away and notify companies such as your bank. Report the incident through ReportCyber and scamwatch.gov.au



You think you have been hacked

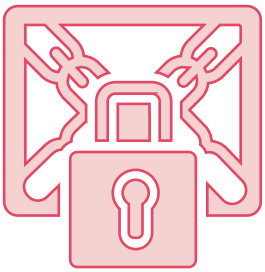
We have developed a tool called 'Have you been hacked?' to help you find out what to do if you think you are the victim of a cybercrime. Visit cyber.gov.au/have-you-been-hacked and report the incident through ReportCyber.



You have fallen victim to a malware attack

A malware attack can have serious and ongoing impacts. If you find malware on your device, stop what you're doing straight away and log out of your accounts.

Report the incident through ReportCyber and scamwatch.gov.au



You have fallen victim to a ransomware attack

Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so you can't access them.

Cybercriminals will demand a ransom to restore access to your files, or to stop them from leaking or selling your sensitive data online. The ransom is usually in the form of cryptocurrency.

If you are a victim of ransomware, don't pay the ransom. Turn off the infected device as soon as possible and follow our steps at cyber.gov.au/ransomware
Report the incident through ReportCyber.

Someone shared private photos or videos of you without your consent

This may include sharing:

- intimate photos or videos of you
- fake photos such as digitally-altered (photoshopped) nudes
- revenge porn
- inappropriate photos tagged with your name
- images of you without your cultural or religious attire.

If the person hasn't shared your intimate details yet, they may be blackmailing you or threatening to do so. If you are uncomfortable and you did not give consent, you should speak up and report it to someone you trust, such as your parent or teacher. There will be help and support for you.

If you are being blackmailed and you are a young person (under 18 years):

- stop all contact with the person
- report it to the Australian Centre to Counter Child Exploitation (ACCCE) at accce.gov.au/report

The Australian Federal Police manages the ACCCE. Any information you provide will help protect other victims and prevent future incidents.

If you are being blackmailed and you are an adult (18 years and older):

- stop all contact with the person
- report it to eSafety at esafety.gov.au/report

If you aren't being blackmailed, still report it to eSafety. The questionnaire only takes a few minutes and will guide you to the right form.

You received unwanted and inappropriate content

You should report it to ACCCE at accce.gov.au/report

Don't respond to the person and block them. This includes someone who is:

- sending nude photos
- saying and doing inappropriate things
- trying to meet in person.

If this didn't happen to you but you saw it happen to someone else, you should still report it.

Someone threatened you, or said harmful things to/about you

Cyberbullying is a very serious issue. You can report it to the platform where it happened and ask them to remove the content.

Each platform is different, so find out what to do for common games, apps and social media at esafety.gov.au
Don't engage with the person and block them.

Someone shared illegal, inappropriate or violent content

You should report any illegal or restricted content, even if it wasn't sent to you.

This may include content that has:

- violence
- terrorism
- sexual abuse
- child exploitation
- self harm.

You can report it to the platform where it happened and ask for them to remove the content. You should also report it to eSafety at esafety.gov.au/report

Each platform is different, so to find out what to do for games, apps and social media, visit esafety.gov.au
Don't engage with the person and block them.

If the content shows physical or sexual violence against children, report it to ACCCE at accce.gov.au/report

Something else happened

If your situation is not listed here or you are unsure, you can contact our 24/7 Hotline on 1300 CYBER1 (1300 292 371). We may ask you to report it through ReportCyber or eSafety.

What if it happened to someone else?

The victim might feel overwhelmed and not know where to start. You could:

- encourage them to report what happened
- report it on their behalf
- ask a trusted adult for help
- share this guide with them.

Before you block an account, it is a good idea to collect some evidence to assist with investigations. You can remain anonymous if you wish. For more information on how to collect evidence, visit esafety.gov.au/report/how-to-collect-evidence

Did you like this guide? Share it with your friends and help them stay safe.

Notes

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre