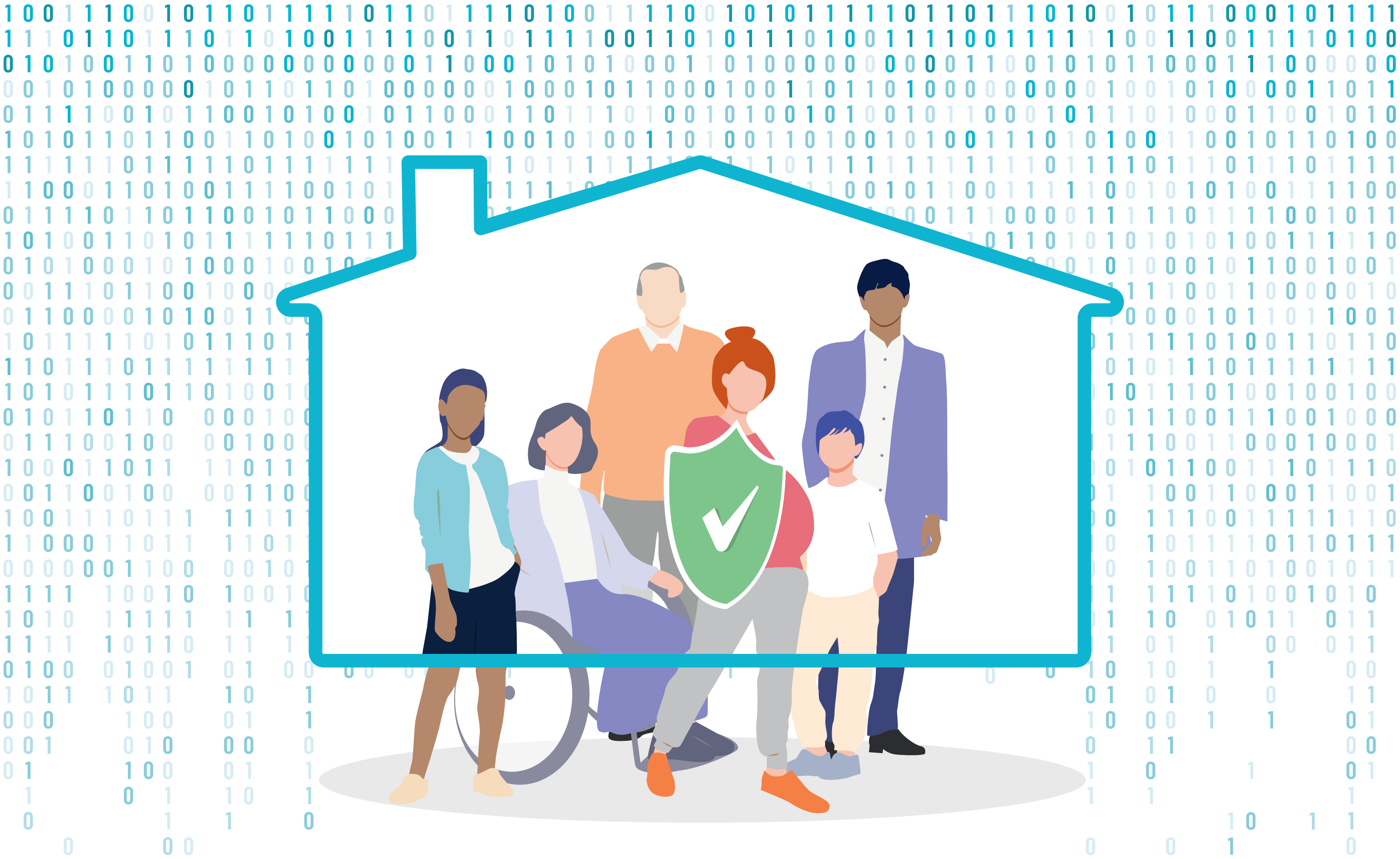
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre



Protect your children online

A guide to cyber security for parents and carers

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

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

PERSONAL
CYBER SECURITY
FIRST STEPS

cyber.gov.au

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

PERSONAL
CYBER SECURITY
NEXT STEPS

cyber.gov.au

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

PERSONAL
CYBER SECURITY
ADVANCED STEPS

cyber.gov.au

Security tips for online gaming

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Security Tips for
Online Gaming

Content Complexity
SIMPLE ●○○

cyber.gov.au

Protect yourself online

Australian Government
Australian Signals Directorate

ASD
ACSC

Protect yourself online

A guide to cyber security for young people

Content Complexity
SIMPLE ●○○

cyber.gov.au

Table of contents

In today's digital age, children are more connected than ever. While the internet provides many ways to learn and socialise, it also exposes children to online threats, such as identity theft and online predators.

As a parent or carer, it is crucial you understand the importance of cyber security. The steps in this guide can help you ensure that your children stay safe and secure online.

Tips for securing accounts and devices

Cybercriminals use a range of tactics to carry out their attacks. Their aim is to steal personal information about you and your family for money and other motives. Let your children know about common online threats to:

- information – stealing passwords to accounts
- identity – stealing personal information to impersonate others
- finances – accessing bank accounts or demanding money.

Below are actions you can take to minimise these risks. If you are still unsure or need immediate help, visit cyber.gov.au/report. If you suspect your child has had a negative experience online, share the 'protect yourself online' advice at cyber.gov.au/families

Create strong passwords or passphrases

Passwords should be private and sharing them can put your data, identity and devices at risk. Children may find it tempting to share passwords with their friends, but this is not cyber secure.

Teach your children to:

- set secure passwords such as a passphrase
- not share or reuse passwords or passphrases.

A passphrase has at least 15 characters using four or more random words. For example, 'purple duck potato boat'. Passphrases are harder for cybercriminals to guess and easy for children to remember.

Involve your children when securing their accounts to teach them good password habits.

To find out more, visit cyber.gov.au/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 accounts from cybercriminals. If someone steals your password, they need another step to access your account.

Turn on MFA for your children's accounts and tell them why it is important.

To find out more, visit cyber.gov.au/mfa

Keep devices and software up to date

The number of published vulnerabilities is on the rise. ASD has reported a 50 per cent increase in vulnerabilities since 2021.

Cybercriminals hack devices by using known weaknesses in systems or applications. Updates from app and software providers have security upgrades that fix these weaknesses.

Regular updates are crucial for keeping your devices secure.

Make sure your children's devices and apps are up to date. Check automatic updates are on and install updates as soon as possible

To find out more, visit cyber.gov.au/updates

Back up your data

A backup is a digital copy of your important data such as photos, videos and documents.

If you lose your data, you can use a backup to restore it. You can create backups using the cloud (a secure way to store data online), or physical media such as an external hard drive.

Backing up your data will put you more at ease knowing it's protected. Think about the impact to your family if you lose your most valued information.

To find out more, visit cyber.gov.au/backups

Disable geolocation services

Geolocation can help you keep track of your children. But, some applications may use or sell location data for commercial purposes.

To stay secure, you can disable geolocation for each app in your child's device settings. Consider deleting apps where this is not possible.

It's best to check apps that your children want to install. Find out what data they collect and turn on relevant security and privacy settings

Sharing family devices

Sometimes you might let your children use your smartphone or tablet. Before you do, consider what type of data, apps and websites you have on it.

Letting a child use your device without security measures can put your family at risk.

Clear your browser history often to limit access to your accounts and private data. Don't share your passwords and PINs with your children. This ensures they have to ask before they use your device or go online.

Bring your own device

Bring Your Own Device (BYOD) is a common trend in schools. BYOD is where children bring their personal devices to class such as:

- laptops
- tablets
- smartphones.

BYOD can have many benefits. It provides more flexibility and access to technology for children at school. But there are challenges, such as ensuring the security and privacy of your children.

Encourage your children to lock their device with a strong passphrase or PIN when not in use.

Ask your children to be careful with what cords or USB devices they use. These can be carriers of malware so it's best to check they are trusted and it's preferred to use their own.

You can also enable a feature to locate and lock the device if it becomes lost or stolen. For more information, search for 'find my' guidance on the device's platform website.

CyberSprinters is an educational game for 7–11 year olds by the UK's National Cyber Security Centre. It also has interactive online security resources and activities. CyberSprinters gives children a head start on staying cyber secure by helping them to make smart decisions. You can play the game with your children and try the puzzles together at home. For more information about CyberSprinters visit ncsc.gov.uk

Social media and gaming

Social media and gaming can be an engaging way to connect with friends, share interests and explore new ideas. But not everyone using social media or gaming platforms are who they say they are.

Gaming

Online gaming has gained popularity among children. It is important to be aware of the potential cyber security risks of gaming.

When playing online games, children may interact with strangers who have malicious intent. Tell your children not to share personal details with anyone they don't know. Cybercriminals could even be impersonating their friend. It is important they are aware of the risks and know they can tell an adult if a stranger contacts them.

Be careful of phishing scams in games. This includes offers of free upgrades, in-game currencies, or rare character items. You should check the source before downloading anything.

Be aware of your child's online activities. You can turn on parental controls on gaming devices and apps.

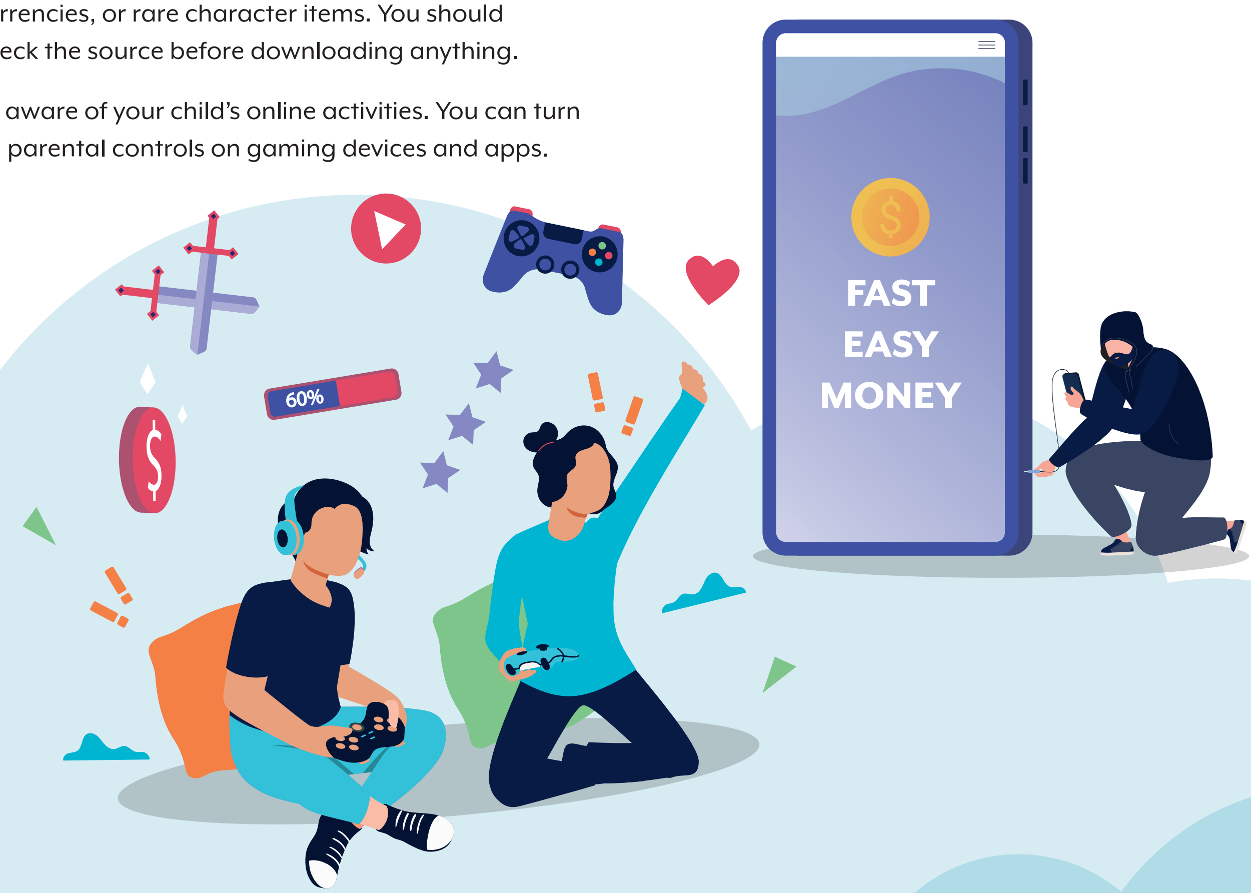
To find out more, search 'gaming' on cyber.gov.au

Social media

If your children use social media, they might have 'friends' or 'followers' they haven't met in real life. Your children might also follow their favourite celebrities or official fan sites.

Many official celebrity and entertainment news websites are safe to use. But it is very easy for people to pretend to be someone else on the internet.

It is important to help your children navigate the digital world to guarantee their online security. Learn additional tips in the next section.



Extra security tips for social media and gaming

Here are some extra security tips for your children when they are on social media and gaming.

- Follow our advice on securing accounts and devices above.
- **Use legitimate software:** Always use apps and games from official and reputable companies. This includes through a trusted physical store, online retailer or app store.
- **Avoid saving payment details:** Where possible, don't save payment details in your 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 a period of inactivity.
- **Be wary of strangers:** Teach your children to check if they know the person online is genuine. If they don't, tell them to ask for help.
- **Be suspicious of unsolicited messages:** This can be a phone call, SMS, instant message, in-game chat or email. If someone your child does not know has contacted them, teach them to ignore this and to tell an adult.
- **Monitor your children's online presence:** Tell your children not to share any personal or sensitive information on social media. For example, their home address or date of birth. Check your child's account privacy settings to know who can see their details. Be aware of age restrictions on social media. Ensure your children understand social media guidelines.

How to recognise scams

Not everyone using social media or gaming devices are who they say they are. By learning how to spot scams and following these tips, you can help your children stay secure online.

You should report scams to scamwatch.gov.au as it helps protect us all from scams.

Be wary of unsolicited requests for personal information

Teach your children to set boundaries for what they share online. You can encourage them to keep their profile private. For example, don't share phone numbers, home or school address, or date of birth. This also includes anything that can reveal these details, such as a school uniform in a photo.

Scammers also often get you to provide financial information or open a file.

Tell your children to block any unusual or or malicious profiles. They can do this by choosing the 'block' option on the user profile, which prevents any further communication.

Check the URL of websites to ensure they are legitimate

When visiting a website, make sure the website address (URL) is the real one. Scammers can create fake websites that look like the real one. This can trick you and your family into giving out their personal information.

Check the domain name (first part of the URL) and spelling is correct. It can be hard to spot since there may only be one letter different.

When making online payments to a bank or store, the URL should:

- start with 'https' (the 's' stands for secure)
- have the company's name in the domain name.

Important: Don't open links or use contact details sent to you. If in doubt, contact the company using details on their official website.

Be wary of offers that seem too good to be true

Scammers might offer something tempting such as a free vacation or money. Remember, if it seems too good to be true, it probably is.

Tell your children to check with a trusted adult before giving out personal details or money.

Recognise the risks

Not everyone online is who they say they are. Encourage your children to take a moment to check if they know the person. Teach them not to visit links or download files from people they don't know. In some cases, a message may appear to be from their friend whose account has been hacked. If in doubt, they should check with the friend offline.

Encourage your children to ask a trusted adult or friend for advice

Your children may not be sure if something is a scam, or someone is asking them for too many personal details. Explain to them to ask for help to figure out if the request is real or fake.

If you are still unsure, it is better to ignore the request than risk losing personal data or money.

For more information on scams in Australia, visit scamwatch.gov.au

The eSafety Commissioner also has resources on online safety basics, privacy and child grooming. Visit esafety.gov.au

Are your children old enough?

Under 5 years old

Children under the age of 5 are still developing an understanding of the world, including the internet. It is crucial for you to supervise and restrict your child's online activity. For example:

- keep devices out of reach and sight
- set up parental controls
- choose age-appropriate content.

Young children don't yet understand the risks of online behaviour. Always be vigilant and don't leave them unattended with electronic devices.

5 to 10 years old

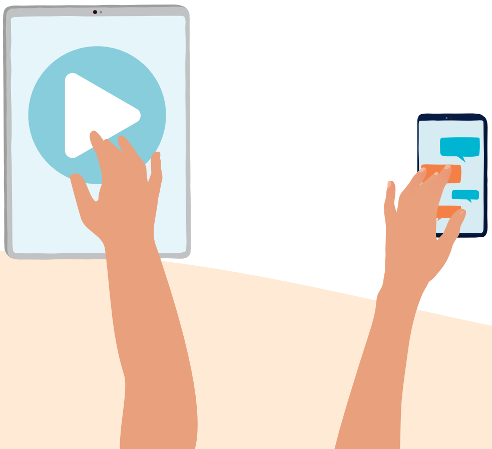
Children aged 5 to 10 are at an age where they are starting to explore the internet on their own. Introduce them to basic cyber security concepts such as:

- use strong passwords
- don't share personal information
- think before visiting a link.

Guide your children to secure websites, games and applications appropriate for their age.

It is important for you to be aware of your children's online activity. If they find something uncomfortable online, encourage them to tell you about it.

Always be vigilant and don't leave them unattended with electronic devices.



10 to 15 years old

As children reach their teenage years, they may start to get into social media and online gaming. This is a good time to introduce them to more advanced cyber security concepts. For example:

- MFA
- how to avoid online bullying.

Teach your children the importance of privacy settings. Make sure they are aware of the potential impacts of sharing personal details online.

Help your children to use technology in a secure way and monitor their online activity.

15 years old and above

Teenagers have more freedom and independence online. This makes them more vulnerable to online threats such as:

- cyberbullying
- scams
- identity theft.

Show your teens how to be secure and to spot suspicious activity online.

It is important for you to have open and honest communication with your teens. Encourage them to talk about their online activity while respecting their privacy.

Try to support them in making responsible choices, especially when gaming and on social media. Make sure teens are aware of the potential impacts of their online actions. Share our guide to cyber security for young people, available at cyber.gov.au/families

Children who are neurodiverse may have specific needs. You should tailor guidance and resources to suit their learning style and pace. For example, use visual aids or interactive activities.

Cyber security checklist for parents and carers

Use this checklist to help your children be cyber secure at all stages of their development.

□ **Set up parental controls on devices:**
This lets you limit what your child can do online and stop them from accessing inappropriate content. Parental control options vary depending on the device and software. Most will allow you to restrict access to certain websites, apps and services.

□ **Talk to your children about online safety:**
Teach them about online dangers such as predators, cyberbullying, scams and identity theft. Encourage them to talk to you about any concerns they have.

□ **Use strong and unique passwords:**
Make sure your children use strong and unique passwords for online accounts, such as a passphrase. Find a reputable and secure password manager to create and store passwords.

□ **Use multi-factor authentication (MFA):**
MFA adds an extra layer of security to online accounts. Enable MFA on all devices and services that support it.

□ **Keep software up to date:**
Update software and operating systems on all devices often. This fixes any security vulnerabilities. Check automatic updates are on and install the update if one is available.

□ **Use antivirus software:**
Check and use antivirus software on devices if applicable. This helps protect them from malware, viruses, and other threats.

□ **Back up important data:**
Back up important data often such as photos, documents and videos. Copy them to an external hard drive or the cloud.

□ **Be wary of online scams:**
Teach your children to be wary of scams and to report them. This includes unsolicited emails, texts, or phone calls that ask for personal or financial details.

□ **Monitor your children's online activities:**
Keep an eye on what your children do online. This includes the websites they visit and the apps they use.

□ **Teach your children to report incidents:**
Tell them to report cyberbullying, or to tell you or another trusted adult. This includes harassment or other inappropriate behaviour.

□ **Stay informed:**
Stay up to date with the latest trends and threats. Sign up for alerts on our website and check the latest scams on Scamwatch. The eSafety Commissioner has online safety resources for parents. You can also access an education program led by the Australian Federal Police, ThinkUKnow.

Remember, cyber security is a shared responsibility. By taking these steps, you can help ensure your children stay safe and secure online. To find out more about these tips, visit cyber.gov.au

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.

Copyright

Use of the Coat of Arms

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