

Protecting your child's identity

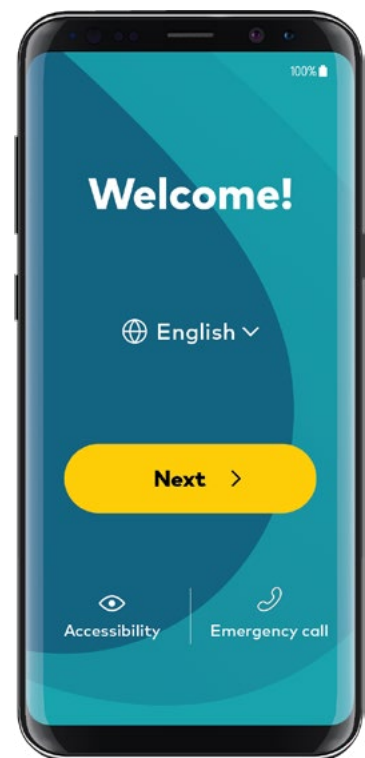
Passphrases, passwords and MFA for your child



Getting their first device is a big milestone for any young person. They will be eager to jump right in, setting up personal accounts to share content and connect with friends. However, these accounts can also give the world access to your child.

As a parent, you want your child to enjoy technology safely. You may feel anxious about their newfound freedom online and think how you can guide them to act in a safe manner.

Start a conversation with your child about the apps, games and social media accounts they want to set up. Discuss the online risks that they might encounter and then work through fun activities as a family to build strong digital defence moves.



This guide will help you talk to your child about:

- ✓ How to create a strong passphrase or password
- ✓ Why you should set up multi-factor authentication where possible
- ✓ Why it's important to protect personal information
- ✓ What to do if they have been hacked
- ✓ Finding more help if you need it



Multi-factor authentication (MFA) is "when you use two or more different types of actions to verify your identify".¹ Using a strong passphrase and multi-factor authentication (MFA) adds an extra layer of protection against cybercriminals and should be used whenever available.

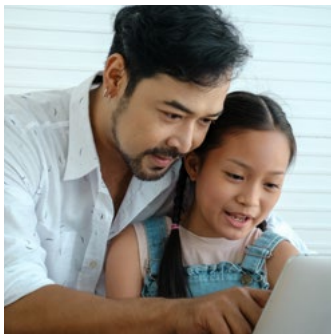
Did you know...



90% of Australians know that it's a risk to use the same or similar passwords...



...but only 31% create unique, strong passwords that are changed regularly.²



Your child is setting up their first gaming or social media account

You want to make sure the platform is right for them and that they can keep their information safe online with a strong password or passphrase



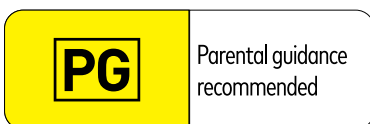
Before they dive into the online world, it's important for you to learn about which games they are interested in to see if it's appropriate for them. Once you know what they want to sign up to, check out the Terms of Service to ensure your child is old enough to participate.

Conversation starter

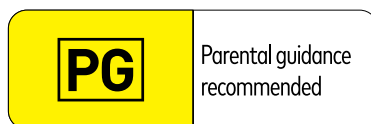
Tell me about the games you want to sign up for. Why do you want to start an account?

Let's make sure this [game is right](#) for you by checking the classification and Terms of Service. This will tell us if you're old enough to use it, and what the platform will do with your information.

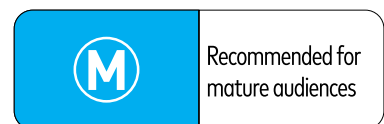
Roblox



Minecraft



Fortnite



For more information about Australian classifications, visit www.classification.gov.au

¹ Protect Yourself: Multi-Factor Authentication | Cyber.gov.au

² LastPass (2020). [Psychology of passwords: The online behaviour that's putting you at risk](#)



Starting an online account means sharing information with your friends, followers or the people you play against. Your child may not understand that sharing certain information may put them at risk or understand how to protect the information they do share on their profiles or in a gaming chat. Protecting personal information is important to keeping your child safe online.

Conversation starter

Personal information is information about who you are or how to find you. Why do you think it's important to protect your personal information?

Have a look at this [list of personal information examples](#) and discuss what someone could do if they knew this about you.

To help protect your child further, encourage them to set their online accounts to private. Together, search the app's/game's settings and see what privacy functions are available such as:

Roblox

Settings	
Privacy	↳
Communication	Custom >
Who can message me	Friends >
Who can chat with me in app	Friends >
Who can chat with me	No one >
Other settings	↳
Who can make me a member of their private server?	Friends >
Who can join me in experiences?	Friends >
Who can see my inventory?	Friends >

Minecraft

Settings	
Profile	↳
Privacy & online safety	↳
↳ This will open up a Microsoft Xbox account:	
Microsoft Xbox account	
Others can:	↳
See your Xbox profile	Friends >
Others can communicate with voice, text or invites	Friends >
See your friends list	Friends >
See if you're online	Friends >
Others can see your activity feed	Friends >

Fortnite

Settings	
Profile	↳
Party joinability	Friends >
Privacy	↳
Matchmaking region	Private >
Language	Private >
Passes	Private >
Mutual Friends	Private >

The difference between passphrases and passwords

To keep your personal information secure, you will be asked to create a password. According to the [Australian Cyber Security Centre](#), using a passphrase where possible is an even better way to help keep information secure as they are more complex and longer than a usual password and therefore can be harder to crack.

A password:

- ✓ Uses a mix of upper-case and lower-case letters, numbers and symbols.
- ✗ Should not include personal information such as full names, date of birth or home address.

A passphrase:

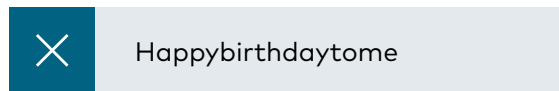
Uses these same rules, but can be stronger because it usually is:

- ✓ **Longer** - Four or more random words and usually more than 14 characters
- ✓ **Unpredictable** - Not a sentence or popular phrase
- ✓ **Unique** - Different for every account

Strong passphrase



Weak passphrase

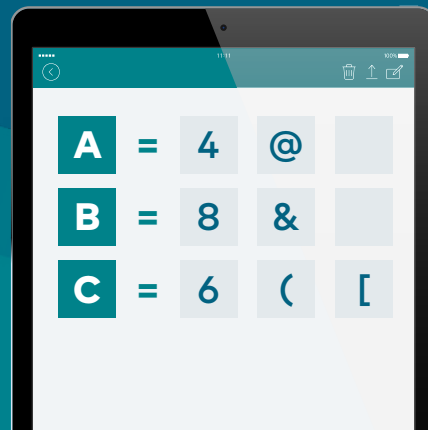


Unique passphrases and/or passwords for every account is an important digital defence move. After using this guide to create strong passphrases and passwords, test the strength of them on [this website](#).³



Activities the whole family can enjoy

To help create strong passphrases and passwords, ask your family to create a number/symbol alphabet by replacing every letter with a number or symbol. Here are some to get you started:



Encourage your child to learn more

It's important for your child to practice their digital defence skills regularly and independently. They can find out more about passphrases, passwords and MFA by reading [this guide](#) and test their digital defence skills by taking [this interactive quiz](#). Practice makes progress, so encourage them to continue to improve their online safety.



[Passphrases, passwords and MFA](#)
- Tween guide



[Passphrases, passwords and MFA](#)
- Quiz

³ Optus is in no way associated or affiliated with the organisation that runs this website.



Excited by receiving their first mobile phone, your child wants to set up a social media account to connect with their friends



This is a great opportunity to talk to your child about upping their online security by enabling MFA where possible on their apps and games.

For more details on setting up MFA on your child's online accounts, check out guidance from the Australian Cyber Security Centre [here](#).

Conversation starter

Do you know which apps let you use MFA? I switch on multi-factor authentication on everything I can! It's like putting a lock on your diary AND putting it in a secret hiding spot.

Why should my child use MFA?

Cybercriminals target adults and kids so it's good to help your child to understand what multi-factor authentication (MFA) is and how to use it where available.

MFA is a login process that asks you for two or more of the following:



Something you know

Passwords, answers to secret questions, keystroke patterns, personal identification numbers (PIN).



Something you have

SMS or PIN (from authenticator or token-generating apps), ID card, bank card.



Something you are

Fingerprints, face, eyes, voice - this is also known as biometrics.

Help strengthen your family's digital defence moves by taking these simple steps:

- ✓ Use MFA whenever you can
- ✓ Only open MFA sign-in links from websites you can trust
- ✓ Update all your household devices with the latest security updates
- ✓ Browse secure websites. A padlock in the address bar or URLs that start with "https" are signs that the website may be more secure. You can often check this before you click on a link, by hovering over the linked text to read where it is trying to send you.
- ✓ Install antivirus software to help protect against malware



Your child tells you that they have noticed someone has tried to log into their gaming account while they were at school

Suspicious login attempts to access gaming and social media accounts are a tell-tale sign of a hacker trying to get access to a personal account. The hacker could be a stranger or someone your child knows in real life. If they can access your child's account, they could use their personal information to put your child in danger.

If someone has this information or hacks your child's account to steal it, they can:



Pretend to be your child



Change your child's posts or profiles



Cyberbully or threaten your child



See or share your child's private pics and personal information



Try to steal your child's personal identity



Your child might struggle to understand the severity of this online risk, so it can help to give examples of online hackers using familiar real-world experiences.

Conversation starter

Hackers want to steal your personal information to...

Which could look like...

Pretend to be you

Someone logging into your account and taking your skins in Fortnite

Change your posts or profile

Someone posting a fake cryptocurrency link from your account and scamming your friends

Cyberbully or threaten you

A fake friend creating a meme from a private pic of you and sharing it with the class

See or share your private pics and personal information

Someone you trusted threatening to share personal pics or information unless you give them money or game credits

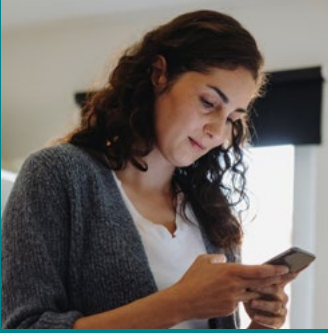
Try to steal your personal information

A stranger getting access to your pocket money to pay for expensive sneakers



If your child suspects that a hacker is targeting their accounts, help them to:

- ✓ Log out of their account and select the option to log out on all their devices – this will log out the hacker too
- ✓ Log back in on to a trusted device
- ✓ Change their passwords to strong and unique passphrases if possible, or at least strong and unique passwords
- ✓ Set up MFA if available to help reduce the risk of this happening again
- ✓ Tell their friends and family of the attempted hack and not to reply to any suspicious messages
- ✓ Ensure their account is set to private so strangers cannot easily contact them
- ✓ Report the incident to the platform



You notice that your child hasn't responded to a message you sent to them in the family group chat



When you see your child, they explain that they have been logged out of their account and can't get back in. They say that they didn't want to tell you because they think it's their fault for leaving their phone unlocked.

Being hacked can be confronting for a child and they are likely to feel scared or embarrassed. Reassure your child that they won't get in trouble or have their device confiscated if they tell you.

Conversation starter

It's a crime to hack into someone's account and steal someone's personal information. You are not alone and it's not your fault. Let's look at what we can do if you think you've been hacked.

If your child cannot access their hacked account, help them through the reporting process:



Contact

The social media or game providers to unlock the relevant account(s)



Keep

Any information that might help – dates they noticed changes, pics and posts, and account names



Screenshot

Any contacts or posts that might possibly be related to the hack or hacker



Report

It to the [Australian Cyber Security Centre](#)

What to do if your child needs more help



For help and support dealing with hackers, check out:

- [eSafety Commissioner](#)
to report cyberbullying, image-based abuse, and illegal and restricted content
- [Australian Cyber Security Centre](#)
to report cybercrime, including online threats and abuse, scams and hacks, data breaches, identity theft and fraud
- [Scamwatch](#)
to report scams
- [IDCARE](#)
to get identity theft, data breach, scam and cyber security support



If your child needs to talk to someone about their feelings or worries, they can contact:

- [Kids Helpline](#)
on 1800 55 1800 for free, private and confidential 24/7 phone and online counselling services
- [13YARN](#)
on 13 92 76 (24/7) for a free, private and confidential talk with an Aboriginal or Torres Strait Islander Crisis Supporter

About Optus Digital Thumbprint

Optus Digital Thumbprint supports digital safety and wellbeing for young people and families. Find out more at www.digitalthumbprint.com.au

