Protecting your child's identity

Stay ahead of scams through family discussions

Scams have changed since our world has gone online. This connectivity makes it easier for scammers to contact us and our family.

We need to prepare our children for the unavoidable exposure to scams, as cybercriminals become more sophisticated and better disguised.

Discuss online scams with your child regularly so they are better protected in their digital environment.

This guide will help you talk to your child about:

- ✓ Why it's important to always be prepared for scams
- ✓ Identifying the most common types of scams and how scammers contact your family
- ✓ Taking steps to protect themselves from scammers
- ✓ Finding more help if you need it

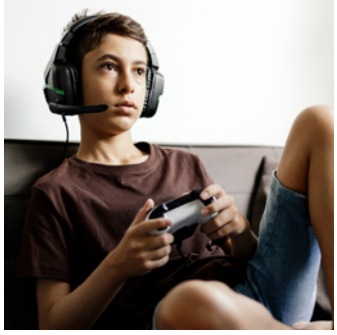
A scam is a way of tricking people into handing over money or personal details.

Online scammers use phone calls, video calls, text messages, emails, social media and gaming platforms to reach their targets.

Did you know...

57% of Australians say they are always wary of phishing and online scams...

... leaving the remaining **2 out of 5** Australians potentially vulnerable.[1]



While your child is playing an online game, they receive a suspicious offer to buy power-ups from another player

While children are statistically least likely to be targets of scams[2], scammers will try to trick young people due to their inexperience with the world and their trusting nature.

Scammers can also deceive people into paying small amounts (i.e. micro-scams) which makes young people prime targets and could lead to something more serious.[3]

Build a healthy scepticism within your child by asking them to question suspicious online activity.

Conversation starter

What happened the last time a stranger contacted you online? Was there something they said that made you question why they were contacting you?

[1] JWS Research report (cyber.gov.au) , p. 37.
[2] Scam statistics | Scamwatch
[3] Targeting scams Report of the ACCC on scams activity 2021 (scamwatch.gov.au)

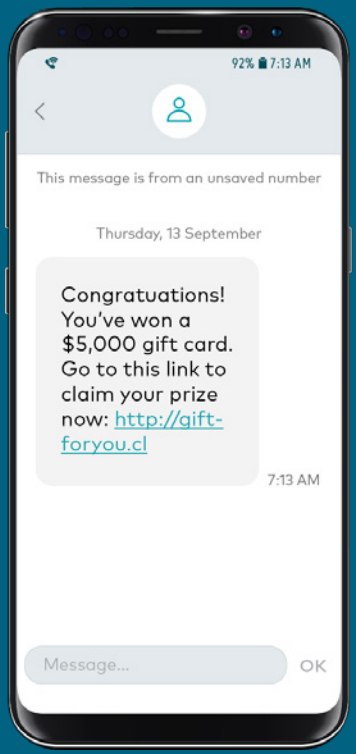
Your child asks for help to sell their bike online, but after asking some questions, you discover that they need money to buy their social media account back from a scammer

Sometimes victims of scams hide that they have been scammed because of the shame or embarrassment they feel about being tricked.

Remind your child that they are not to blame if they are scammed and share a story of a time you or someone you know were scammed.

Conversation starter

When I was scammed online, I felt embarrassed even though I shouldn't have to. Can you think of a reason why I felt that way?



Scammers might use digital blackmail or extortion methods, such as deploying ransomware on a victim's device, then make demands that their victim to pay them money. This can be an extra layer of humiliation that might prevent the victim from telling someone.

Encourage your child to speak up and take action if they have been scammed. Let them know that you 'have their back' and will always support them.

Conversation starter

Extortion is a particularly nasty way scammers get money. They get something we value and demand money in exchange for it. What are some things we need to protect?

What are the most common types of scams?

Investment

These scams tempt the victim with a small investment of money or information that promises bigger gains in the future. They prey on an individual's eagerness to earn money quickly.

Sign up to our Beginners Guide to Crypto course and get a free bitcoin token.

Penalty

The scammer adopts an authoritative persona, such as a person from the accounts team at a social media or gaming platform, and threaten consequences if they are not paid.

Your payment didn't go through for your latest power-ups so we will have to cancel your account unless you pay now.

Prize

This type of scam is easy to get swept up in because the target is told they have won something. But to claim the prize, the target must send money or personal information.

You have won our weekly jackpot! To receive your winnings, we need your bank account details.

Shopping

Shopping scams can often focus on the target's need to find a bargain or quite the opposite. The scam might involve a very rare item. Either way, the scammer will not send the target the purchase when paid upfront, instead they have deployed a phishing link or gathered personal information.

Here's your only chance to get 95% off designer sunglasses. Just click the link.

Charity

Scammers use a cause – real or fake – that appeals to their target's compassion.

I'm collecting money for the endangered drop bear, would you kindly donate?

Computer

Often the scammer will contact their target and gain remote access to their computer to get personal information or install malware.

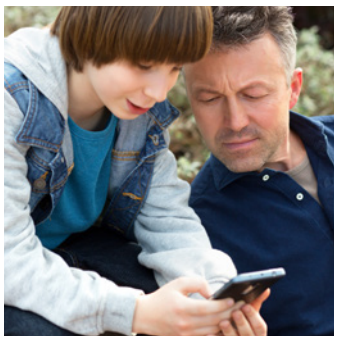
Your computer is infected by a virus, but we have our tech team on standby to remove it. All I need is access to your computer.

Sexual extortion

Also known as 'sextortion', these scammers coerce their targets by claiming that they possess intimate images or videos of their target and demanding payment so that they would not share the content to people their target is close with.

I will leak your image/ video to everyone you know if you don't pay me in 24 hours.

Scams are always evolving in different ways, so be sure to keep an eye out for the latest scams by visiting Scamwatch.



Your child shows you a direct message from an online friend and is worried that they might mistake genuine online activity with a scam

Remind your child that it's better to be suspicious and get it wrong, than end up being scammed.

Explain the G.A.P.S checklist to help your child spot a scam.

G

Gain trust:

Scammers might say they are from a legitimate organisation or impersonate someone familiar to make them trustworthy. Check to see if they are who they say they are.

A

Appeal to your emotions:

Scammers know that their targets are more likely to help them if you feel bad for them or really like them, so they might lie about sick pets or family members, or give loads of personal compliments. Acknowledge these feelings but refocus on suspicions.

P

Procedure change:

Scammers will insist on using their own verification procedures, such as sending their target to a new website or phone number. It might feel or look identical to the authentic procedure so refocus on suspicions and stop the procedure.

S

Speed:

Scammers create a sense of urgency to get their targets to make decisions without thinking them through. If they say you need to act now or that the offer expires today, wait until you have done your own research into the offer.

Conversation starter

What if someone contacted me online and said they were from my work. They say they're a new employee and don't know the correct process, but they need me to check a document by tomorrow and sent me a link to open it. Let's use the G.A.P.S checklist to see how I should respond.

You noticed a new program on your child's laptop

When asked, your child tells you that tech support from their favourite game contacted them to trial a new version of the game. They downloaded the file, but it didn't seem to open. They also sometimes notice their cursor moving without them controlling it.

Scams can catch us off-guard and sometimes we might not even know we are experiencing a scam. Scammers can use 'malware' – malicious software – to gain access to your devices and personal information.

Some signs that you or your child are actively being scammed are:

- Your device is performing actions that you have not initiated, or you notice the cursor is moving without you moving it
- Unknown transactions appear on your financial statements
- Strange messages are sent from your child's social media or email account to their contacts (often includes a phishing link)
- You receive a notification of a login attempt or you are locked out of your computer or online accounts
- Apps or programs that you did not download are installed on your device
- You have not received promised money, products or services

What to do if you are being scammed

Stop all contact with the scammer

Remember to collect evidence before exiting a chat or blocking the scammer.

Change all passwords and passphrases

Learn more about creating strong passwords and passphrases here.

Don't pay and don't give into their demands

Scammers are cybercriminals who might be using the money they gain to enable illegal activity.

Collect evidence and report it

Screenshot or screen record any interactions with the scammer to report it to the authorities and tell your online contacts to be on alert. Do not screenshot intimate images or videos as it can be a crime, especially if the person is under 18. You can take screenshots or recordings of when and where it was shared.

What else can you do?

Talk to your child about the actions they can take that can help them fight off scammers.

Awareness is key

Keep the conversation going about new scam tactics you may hear about.

Conversation starter

What is the latest scam you have heard about or seen online?

Familiarise yourself

Get to know who you are dealing with.
If the message feels suspicious:

- ✓ Research the stranger sending it
- ✓ Investigate the legitimacy of the organisation
- ✓ If it is your online friend, contact them on a different platform to see if their account has been hacked

Conversation starter

What disguise can a scammer use to approach you?

What would you do if you were sent suspicious link by a stranger? An organisation? An online friend?

Do not click the link

The easiest way a scammer can install malware and capture your personal information is to get you to click a link. Report and delete any suspicious links.

Conversation starter

Can you think of a time a someone sent you a suspicious link via email or messaging app? How did you know it was suspicious?

Go private

Set your child's social media and gaming accounts to private and remind them to keep their personal information offline.

Conversation starter

Let's look at your social media profile. What information do you think could be used by a scammer?

Check payment is secure

The scammer is almost always after money so be extra cautious at time of payment.

- ✓ Research and read reviews about the retailer to ensure they are legit
- ✓ Check the URL begins with 'https' and the address bar has a closed padlock next to it
- ✓ Avoid upfront payment via direct deposit

Conversation starter

How can we shop safely online? Can you give me any examples of suspicious things to avoid when online shopping?

What to do if your child needs more help

Take action by contacting:

- eSafety Commissoner
  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
- Australian Centre to Counter Child Exploitation
  to report online grooming and inappropriate contact
- IDCARE
  to get identity theft, data breach, scam and cyber security support

kids help line

13YARN
"Our Story, Our Healing"

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

Trusted eSafetyProvider
esafety.gov.au