Protecting your child's identity

Recognising hackers, scammers and fake friends

Connection to the digital world feels like a necessity in the everyday lives of Aussie children. As digital natives, they are keen to set up accounts to share content, meet friends and participate in online gaming communities.

While connecting online can have many positive impacts, it's important to have an ongoing conversation about the risks of the digital world.

You can help young people avoid veering into the path of cyber criminals by showing them some simple digital defence moves.

This guide will help you talk to your child about:

- ✓ Why it's important to be suspicious of online strangers and fake friends
- ✓ Identifying the different types of cybercrimes
- ✓ Improving digital defence skills
- ✓ Where to find more help if they need it

Hackers are cyber criminals who may break into your accounts or devices to get your personal information. Some use software called malware (short for malicious software).

Scammers may trick you into giving them your personal information. Some use malware or phishing links.

Fake friends may have bad intentions with using your personal information, even if they are already close to you in real life.

Did you know...

While children are the least likely to report being scammed[1] ...

... recently there has been a 100-fold increase of reports of Australian children experiencing sextortion[2]...

...and authorities speculate the number of victims is much higher.

Your child shows you an email they received saying that their gaming account is going to be shut down, but it can be reinstated if they click a link

Scammers will use phishing links in fake emails to try to trick the account holder into revealing personal information about themselves.

The link takes the victim to a website that appears to be genuine but asks for bank details, account names and passwords among other personal information.

Online criminals target young people who may not understand how valuable their personal information is and the risk in exposing it.

Conversation starter

What should you do if someone you don't know sends you a strange-looking hyperlink or requests to connect online?

[1] Scam statistics | Scamwatch
[2] AFP and AUSTRAC target offshore sextortion syndicates preying on Australian youth | ACCCE

Digital defence move #1

Stay scam-aware

Remind your child about different scams out there to build their scam awareness. Check out the Stay ahead of scams family guide here.

Stay ahead of scams
- Family guide

Your child is upset that an older student at their school is sharing personal information about them online

Your child is confused and hurt by this because they thought they were friends.

Doxing is a form of cyberbullying that involves sharing the victim's personal information without their consent to intentionally harm them. They may find this information through hacking, talking to other people, talking to the child themselves or tricking them in some way.

Remind your child that even if they've met someone in real life, they don't need to engage with them on social media or online gaming. Someone who they've met once at school, a party or through sports could still want to find out information to use against them.

Conversation starter

Can you think of a time when someone you met or knew in real life added you online, but you didn't want to accept? Why not?

Why might you choose not to connect with someone online, even if you've met before?

Digital defence move #2

Use MFA

Use strong passphrases/passwords and set up multi-factor authentication for their social media or gaming accounts. Check out the Passphrases, passwords and MFA family guide here.

Passphrases, passwords and MFA
- Family guide

A concerned parent shows you a social media account that uses your child's image and personal information to be mean to their child

Your child insists that they don't own the account.

Catfishing is when someone uses a fake profile to contact their victim, either to bully or extort money or scam their victim. This type of cybercriminal creates fake profiles using images available to them online and they will create a back-story that fits the images.

If they have a specific target in mind, they may use any personal information also available to them to make it as realistic as possible. In some cases, catfishers will hack a victim's account to bully or extort or scam others.

It's important not to discourage your child from the online world entirely, but help your child understand that their personal information is valuable to online criminals.

Conversation starter

Using a fake profile to bully someone online can have big consequences.
How can we protect our online information from catfishers who might use our image to hurt people?

Digital defence move #3

Stay private

Regularly review and check your child's privacy settings on their social media and gaming accounts. Check out our Safeguard your child's privacy guide here.

Safeguard your child's privacy
- Family guide

You notice your child mentioning a new friend that you don't recognise from school

Your child seems very close with this person but finds out they are almost double their age.

Predators can easily hide their real identity and build fake friendships with young people through shared interests online. If their older fake friend has sinister motivations, your child could be a victim without knowing it.

Capping is a term used by offenders that involves attempts to capture or screenshot (screen-cap) sexually explicit images of young people while they on live stream or video, often without their knowledge.

Young people are more likely to tell you when they encounter unwanted contact if they feel they won't be judged or punished for doing so. Try to help your child understand in a way that is age-appropriate, that they are vulnerable to predators who pose as fake friends.

Conversation starter

How would you feel if you found out that the person you are talking to online is not who they say they are? Why do you think a stranger wants to pretend to be someone else and connect with you?

If you are unsure about someone contacting you online, who should you talk to?

Digital defence move #4

Block randoms

Explain to your child that they should block or remove followers and accounts that are unwanted. Check out the Blocking unwanted contact family guide here.

Blocking unwanted contact - Family guide

You find intimate images of your child on the family cloud account

When you talk to them about it, they are visibly upset, and explain that someone threatened to share secrets about them if they didn't send them the images.

Sextortion is a type of blackmail online criminals use to extort money from their victims. They threaten to share intimate images they have obtained from their victim unless their demands are met.

The intimate images could be obtained by hacking their victim's account or establishing a fake friendship that convinces the victim to freely share the images.

Begin with reminding your child that it's not their fault this has happened and that you always have their back when it comes to protecting them online.

Conversation starter

Your feelings are valid and by telling me more about the situation, I can help. Let's look at what we can do next to stop this now and protect you in the future.

Digital defence move #5

Speak up

Victims think they will get in trouble if they speak up and report it. This is not true and children are never to blame for being a victim.

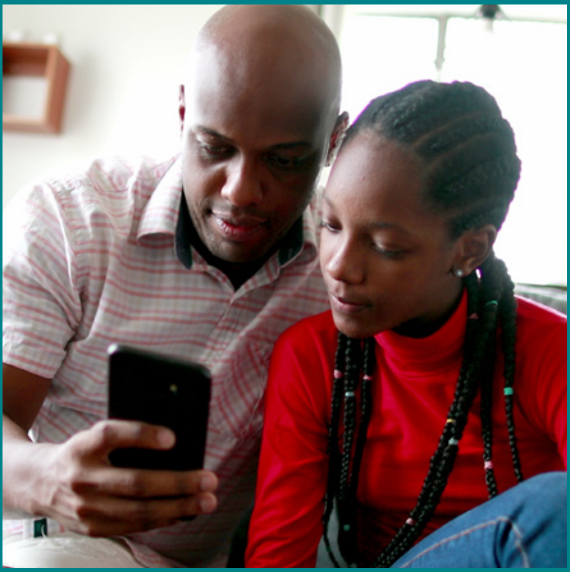
Digital defence move #6

Report it

Together with your child, report it to the platform and seek help from the app, gaming service providers or authorities.

Do not screenshot the actual image or the video as it can be a crime. You can take screenshots or recordings of when and where it was shared.

What to do if your child needs more help



Take action by contacting:

- 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
- Australian Centre to Counter Child Exploitation
  to report online grooming and inappropriate contact
- IDCARE
  to get identity theft 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 for a free, private and confidential talk 24/7 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 eSafety Provider
esafety.gov.au