Scams

Impersonation scams

A scammer may be an anonymous person or someone pretending to be

- from a social media platform
- from a company doing security checks for a platform
- a Government department
- Victoria Police

They may ask you (or your child) to:

- Confirm personal details/identification
- Open an email
- click a link directing you to a fake website
- provide your account username and password
- send or upload identity information such as passport, driving licence or proof of age card
- record videos of yourself to prove your age
- pay a fine for being on a social media platform while under 16.

Buying and selling scams

Someone may offer your child a fake ID or direct access to an age-verified account. They may collect personal information and say your child has to pay them money or do something for them, like sending nudes or being sexual online.

It is important that your child DOES NOT PAY or send anything (photos, videos, reply messages) – it may be a scam, 'sextortion' by someone who plans to blackmail them, or 'grooming' by a sexual abuser.

It's unlikely they will provide what they've promised, or if they do provide access/links that work, they may threaten or blackmail to report your child, unless they are sent more money or content.

IMPORTANT: Do not block the account – contact the police immediately and they can support with shutting down the account and/or taking it over to catch the perpetrator.

Account takeover scams

Scammers send messages using a fake profile with a profile photo of someone you may know. They request may request a phone numbers or email address access and for example, state they have lost their phone (or they don't have one) and just need to use child's phone number to get a verification code. They may claim this is because they've been asked to log back into their own social media account to prove their age.

But the message is not really from your child's friend – that friend's account has been hacked by a scammer. Now the scammer will use the verification code to log into your child's account and change the password. They may then say your child has to pay them money to get back control of their account.

'Hi Mum' style scams

You may receive a message from a scammer pretending to be your child. For example, they may claim they've lost their phone, so they're using someone else's number.

They may tell you:

- you need to click a link to verify their age
- they need you to send copies of their identity information (such as a passport, proof of age card and/or birth certificate) so they can verify their age (or get back into their account).

Further support

To find out more about the latest scams and how to protect yourself, check the Australian Government's ScamwatchExternal link website.

Being scammed is a horrible experience, and it can happen to anyone. If your child needs someone to talk to, they can reach out to Kids Helpline (for 5- to 25-year-olds, 24/7) or counselling or support services.

You can also reach out to IDCareExternal link, a not-for-profit organisation that can help you recover from scams, identity theft and other cybercrimes.

Someone has offered to help my child get around the age restrictions of social media. Is that a scam?

Yes, it could be a scam.
The scammer may be after money or personal information. Or they may want to send nudes or get sexual online – this can be 'grooming' by a sexual abuser, or a set up for 'sextortion' by someone who plans to blackmail over the sexual content.

If someone says they will give your child a fake ID or direct access to an age-verified account, the advice is:

- DO NOT PAY
- DO NOT send them nudes or get sexual with them online
- DO NOT send personal information that could be used to access your accounts or steal your identity.

This means that if a child under 16 years of age receives a request to pay a fine for being under 16 or for not having a verified account, it's a scam – DO NOT PAY. (See ScamwatchExternal link)

There's no mandatory reporting of users under 16 – for parents, educators or police. However, reporting use by an child under 16 may help the platform to understand how they're getting around age checks, so it can tighten safety protections for all.