Protecting teens from online scams

internet matters.org

How to keep scammers from targeting your child

Learn to **recognise** risk, **react** in appropriate ways and **resolve** issues caused by scams online.

Recognise

- **Talk about common scams that often target teens**, such as online shopping scams, fake giveaways or phishing attempts.
- Emphasise the importance of **ignoring requests for personal information.** To protect their privacy they should also approach online forms in shops or for competitions with caution.
- Encourage them to **check URLs, reviews and comments for shops** to make sure they're buying from reputable sources and that the information they see is legitimate.
- **Explain how scammers can use AI** to create convincing fake videos or voices. Encourage them to **fact check before sharing** or providing any details.

Talk about sextortion and general extortion as well, and the importance of blocking people who threaten them or make them uncomfortable. Encourage teens to tell you if this happens.

React

- Empower them to **follow their instincts;** if something seems 'off', it probably is. **Block or report users.** Or ask a trusted adult for a second opinion.
- Encourage them to **report suspicious posts on social media,** even if they're not the target. If the scam is well-known, they can also **speak out in the comments to warn others if it's safe to do so.**
- Together, **review the blocking, muting and restricting options available** in the apps they use or games they play, and encourage them to make use of these features.
- **Create a secret word together** and encourage teens to do the same with friends or other family members. If someone pretends to be a person close to your teen, a secret word can set imposters apart from real family or friends.
- **Regularly check-in with your teen** about the content and people they interact with online to help you identify potential risks. Supervised or teen accounts on social media can help with this.

Help them run regular security checks by ensuring their device has cyber security software installed.

Resolve

- If your teen becomes a victim of someone's scam, show them **how to make a report on the platform** and contact the platform's support team if necessary (such as if they've lost access to their account).
- If someone scams your child or sends messages that could lead to scams, **encourage them to make a report to ActionFraud or the IWF**, especially as the same scam can target someone less prepared.
- In the case of financial scams, **contact your teen's financial institution** or card provider to limit long-term issues.
- If they share personal information, help them **change their passwords and consider using a password manager.** Set their **profiles to private** and involve them in any other security updates
- Remind them that anyone can become a target and victim. **It's not their fault,** but you can only help them make it right if they tell you about it.

Talk with your teen about the issue in a calm way. Ask them about what they could do differently in the future and talk through their worries with them.

Scan or visit **internetmatters.org** for more advice

InternetMatters
@InternetMatters
@internetmattersorg
@im_org
Internet Matters Ltd
@internetmatters.org