# Protecting 6-10-year-olds 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 to children about **common 'red flags'** such as messages that promise free gifts, other users asking for passwords or personal information or pop-ups that tell them to 'click here'. If these come up, encourage them to **tell you right away.**
- Teach them to **think critically** by using realistic examples like, "What would you do if a stranger came up to you in the park and asked you for your home address? Or if they offered free sweets?" Encourage them to **block online users** who ask for personal information or offer free things.
- Explain that pop-up ads in their games might seem trustworthy but can hide scams behind them, so they should **avoid clicking/tapping** on them. If they accidentally click on them, they should tell you so you can check the device.

**Additionally, some ads or users might offer cheat codes, free in-game currency or other free items. These are often scams, so remind children to not click on these or tell you if they do.**

## React

- **Encourage them to tell you** if something seems odd or they see a suspicious message.
- Show them how to use **report features in games or apps** to flag content or users that might promote scams.
- **Create a secret word** together and with others in your child's life. If someone contacts your child and says they are family member or family friend, your child should ask for the secret word. If the person can't give the secret word, your child should tell you.
- You should **regularly review** the games your child plays and the videos they watch, including their watch history or screen time reports. This can help you identify potential risks.

**Remember to run regular security checks as well. You can do this by ensuring their device has cyber security software installed.**

## Resolve

- If they do click on something suspicious like a pop-up ad, get them into the habit of **telling you so you can check the device** for threats.
- If they find themselves somewhere that makes them feel uncomfortable in anyway, encourage them to **leave the space and tell you.** If a user is making them uncomfortable, they should block and report them.
- Depending on what the stranger says to them, consider making a report to ActionFraud or the IWF.
- If they share personal information, help them **change their passwords** or make their profiles private.
- Reassure them they **won't get in trouble for coming to you** – it's always better to share what happened so you can help.
- Talk to your child about the situation **calmly and openly**. Discuss what they might do differently next time, and take time to address any worries or concerns they have.

**You might also want to review the parental controls you use to see how you can minimise an incident in the future.**

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

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