

Online Safety News

July 2024



Snapchat 13+ what are the risks

Snapchat is one of the most popular social media channels with young people. It has an age rating of 13+ but there is no age verification process in place so it is easy for younger children to create accounts.

The Risks of Snapchat for children:

- **There is a lot of adult content on Snapchat,** Inappropriate or harmful content. Much of this will just appear on their Discover Feed.
- **Location sharing:** Snap Map shares your location with other users on the app.
- Your child could receive **unwanted contact** from other users on the platform
- **Disappearing messages** can make children feel that it is ok to share inappropriate pictures or messages because it won't last. This is not true. Messages can be screen shotted and shared elsewhere.
- **Pressure to respond/chat** - with 'streaks' there is a pressure to keep using the app to achieve a higher 'streak score' with their friends.
- **Parental controls are minimal** and can easily be deactivated by the child.
- **There is a secret vault called 'For My Eyes Only'** My Eyes Only is for Snaps that you want to keep extra private and a separate passcode is created to access the vault. Not a feature many parents would want their child to have.
- Cyberbullying and a culture of FOMO (Fear of missing out) is also very prevalent on snapchat.

In Summary: Common Sense Media recommends an age of 16+ for Snapchat. It is not a safe app for younger children.

Is your child talking to strangers online?



- ***"A survey of almost 4,000 children found that 43 percent of those aged between 8 and 13 years old are talking to people they have never met in real life on social media and gaming platforms". (Savvycyberkids.org)***
- More than half gave their phone number to a stranger online
- 1/5 spoke with a stranger on the phone
- 11% went as far as meeting someone

Children can easily give away too much information online and be too trusting. It's important we talk to children about the risks of strangers in real life AND online.

Make sure any accounts or profiles your child as are set to private and that they understand the importance of not sharing personal information online.

Questions to ask:



- Have you ever shared your password with anyone? How could you fix it?
- What is your personal information?
- If a stranger found your social media profile or on a game - what can they see or find out about you?
- Why should we only connect or chat to people online that we know in real life?

Harmful Online Challenges

Internet Matters have launched the 'Be Challenge Aware' campaign in partnership with Lisa Kenevan and Hollie Dance, who both lost their sons to dangerous online challenges. They share their advice and tips with Internet Matters to help protect other children from harmful online challenges.

Internet Matters have also included links to further resources regarding online challenges at the below link:

<https://www.internetmatters.org/hub/parent-stories/tips-protectchildren-harmful-online-challenges/>

In - App purchases and how to turn them off

In app purchases are a form of digital purchasing where users can buy items, services or features **within an app**.

A typical example would be, if you play a game on your phone that allows you to purchase specific upgrades like tools or clothing to upgrade your character's capabilities, that would be an in-app purchase.

What are the risks?

- Children having unauthorised access to real money, such as credit or debit cards, PayPal accounts, and even gift cards when it's linked directly to an app store account. With each purchase, there is the potential for users (especially children) to accidentally spend large amounts of money without realising it.
- Unmonitored access to in-app purchases can leave children vulnerable to fraud, identity theft, and other security breaches. Often, children may not fully understand that these are real sources of funds, making them more likely targets of scams or data theft.
- Often there is unrestricted access to virtual goods or content without parental participation. This can allow young users to engage with inappropriate or harmful content, or enter unsupervised chat rooms, which can lead them towards online predators.

How to turn off In-app purchases:

On iOS devices

1. Tap the settings icon on your child's device.
2. Tap Screen Time, and enable if not already turned on.
3. Scroll down and tap Content & Privacy Restrictions.
4. Toggle on Content & Privacy Restrictions.
5. Then, tap iTunes & App Store Purchases.
6. Tap In-app Purchases.
7. Tap Don't Allow.

On Android devices

1. Open the Google Play Store app on your child's device.
2. Look for the icon in the top right corner of the screen and tap it.
3. From the pop-up menu, tap Settings.
4. Tap Authentication from the Settings page.
5. Next, tap Require Authentication for Purchases.
6. Select For all purchases through Google Play on this device.
7. Have your child's Google password ready to enter, if asked. You may want to change it to one only you know so they can't change your settings.

