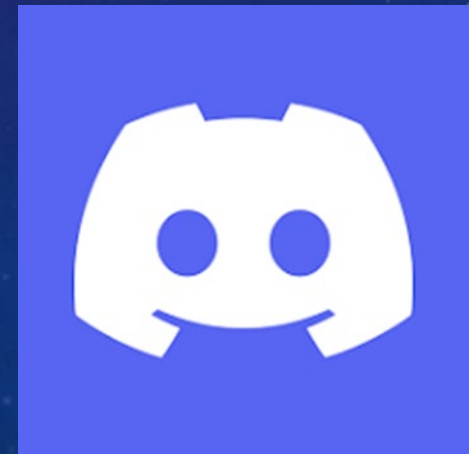


Social Media



Social Media



Risks

- Public profiles expose children to strangers.
- Algorithm may show explicit or harmful content.
- Dangerous or inappropriate viral trends.
- Messages via DMs or comment threads can't always be monitored.

Steps to Stay Safe

- Set account to **private** and **review followers** regularly.
- Enable **Family Pairing** to control screen time and messaging.
- Turn on **Restricted Mode** to filter mature content.
- Have open discussions about **online trends** and how to respond.

Social Media



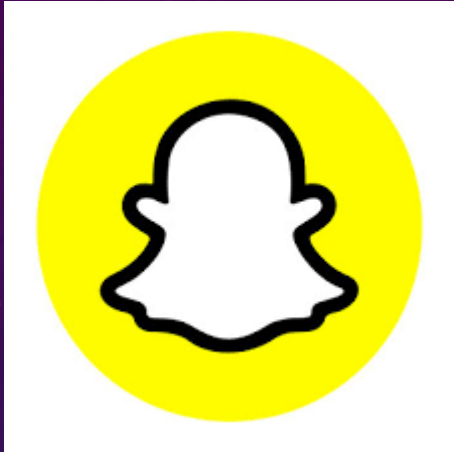
Risks

- Public profiles allow strangers to follow or message.
- **Disappearing DMs** and secret “Finsta” accounts.
- Body image and lifestyle comparison pressure.
- Inappropriate or explicit comment sections.

Steps to Stay Safe

- Make the account **private** and turn off **location tagging**.
- Adjust **message and comment settings** to limit exposure.
- Follow only **real-life friends and trusted accounts**.
- Talk regularly about **online image pressure and boundaries**.

Social Media



Risks

- **Disappearing messages** make monitoring difficult.
- **Snap Map** can reveal real-time location.
- Pressure to maintain **streaks** leads to excessive use.
- “Quick Add” exposes kids to unknown users.

Steps to Stay Safe

- Set Snap Map to **Ghost Mode**.
- Limit who can contact them in **Privacy Settings**.
- Review their **friend list** together occasionally.
- Explain that **disappearing Snaps** can still be screenshotted or misused.

Social Media



Risks

- **Age-inappropriate videos** can bypass filters.
- **Comments** may include adult content or predators targeting minors.
- **YouTube Shorts** often include mature themes.
- Algorithm may guide kids toward **increasingly extreme content**.

Steps to Stay Safe

- Use **YouTube Kids** or enable **Restricted Mode**.
- Turn off **autoplay** to reduce uncontrolled viewing.
- Review their **watch history** and subscriptions regularly.
- Use tools to **limit screen time and access**.

Social Media



Risks

- Children can join **unmoderated public servers**.
- **Direct messages from strangers** may include grooming attempts.
- **NSFW content** is accessible even with age restrictions.
- Voice/video chat makes predatory interaction easier.

Steps to Stay Safe

- Disable **DMs from non-friends** in settings.
- Check and leave **inappropriate servers** with your child.
- Turn off **NSFW content** in user settings.
- Set clear expectations for **online communication** and report violations.

General Key Points

- Set accounts to private
- Disable location sharing
- Discuss what's okay to post
- Monitor friend lists and followers
- Use monitoring tools - <https://www.internetmatters.org/advice/apps-and-platforms/monitoring/>
- Encourage open conversations, not fear

Gaming



Gaming

Risks – Games Kids Use & How Exploitation Happens

- Games: Fortnite, Roblox, Minecraft, Call of Duty, Among Us
- Dangers: In-game chat, grooming in multiplayer spaces, toxic behaviour, addiction
- Microtransactions & gambling elements (e.g., loot boxes)

How to Stay Safe – Gaming

- Enable parental controls on consoles/devices
- Use child accounts (Xbox/PlayStation/Roblox)
- Turn off chat or restrict it to friends
- Talk about online strangers and fake identities
- Set time limits and gaming curfews

Cyber Bullying

Risks – What It Looks Like

- Harassment, exclusion, doxing, impersonation
- Happens on Snapchat, WhatsApp, group chats, TikTok comments
- Often hidden from parents due to shame or fear

How to Stay Safe – Bullying Prevention

- Teach kids how to block/report
- Encourage them to screenshot and talk about issues
- Know signs: withdrawal, changes in mood or sleep
- Involve school if necessary
- Keep digital evidence (but don't retaliate)

Exploitation

Risks – Tactics & Platforms

- Grooming often happens on Instagram, TikTok, Discord, games like Roblox
- Tactics: flattery, shared interests, gifts, threats, blackmail (sextortion)
- Offenders may pose as teens or use fake profiles

How to Stay Safe – Preventing Exploitation

- Teach kids red flags: secrecy, quick emotional connection, gift offers
- Set rules about private chats and video calls
- Watch for signs: secrecy, mood changes, use of burner accounts
- Encourage your child to say something *even if they're scared or feel "at fault"*

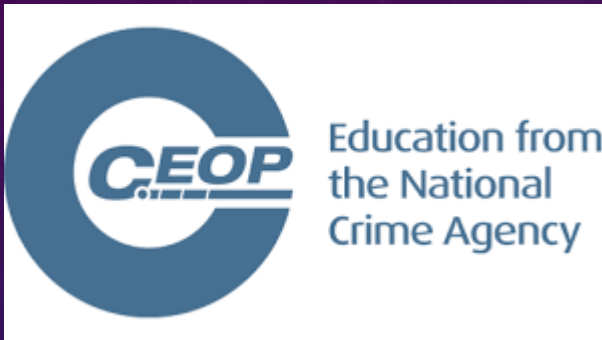
Artificial Intelligence (AI)

- **Fact-Checking** – Teach kids not to trust AI-generated content blindly and verify information.
- **Personal Data Protection** – Ensure they understand not to share private details with AI tools.
- **AI Chatbots** – Explain that AI responses may not always be accurate or safe.
- **Deepfake Awareness** – Educate them on manipulated images and videos that can spread false information.
- **Ethical Use** – Guide them on using AI responsibly for learning, not for cheating or harmful purposes.

Digital Footprint

- **Permanent Posts** – Teach kids that what they share online stays forever.
- **Online Reputation** – Help them understand how their digital history can impact future opportunities.
- **Secure Passwords** – Encourage strong, unique passwords for all accounts.
- **Be Mindful of Sharing** – Avoid posting personal details like addresses or school names.
- **Review Regularly** – Go through their online presence together and remove anything inappropriate.

Resources



- ACTION ONE

Your passwords should be long, strong and not duplicated across your other accounts.

Combining 3 random words that each mean something to you is a great way to create a password that is easy to remember but hard to crack.

Do not use words that can be guessed (like your pet's name). You can include numbers and symbols if needed. For example, "Hippo!PizzaRo&cket1"

Use a password manager!

ACTION TWO –

2-Step Verification (2SV) – a second way to confirm your identity

It gives you twice the protection so even if cyber criminals have your password, they can't access your account.

2SV works by asking for more information to prove your identity. For example, getting a code sent to your phone when you sign in using a new device or change settings such as your password.