

Keeping Your Child Safe Online: A Simple Guide for Parents and Carers

Keeping children safe online is just like keeping them safe in the real world. You do not need to be an expert with technology to help them.

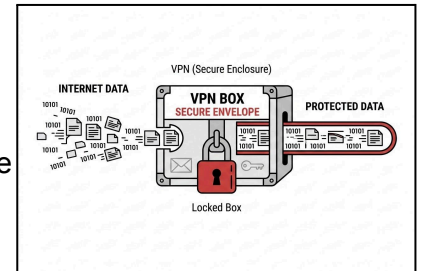


1. What is a VPN?

A VPN is a secret envelope for the internet.

Normally, internet use is like a postcard. You and your internet provider can see the details and keep your child safe.

A VPN puts that postcard inside a locked box.



- **Why children use VPNs:** To unblock games, videos, or websites that are blocked at home or school.
- **The danger:** Home safety filters cannot see inside the locked box. Children can see scary or adult content even with safety controls on.

What to look for: Check their device screen for apps with a key, padlock, or shield icon.



2. What is the Dark Web?

Think of the internet like a shopping center:

1. **Main Shops (Normal Web):** Google, YouTube, BBC News. Bright, open, and safe for everyone.
2. **Staff Rooms (Private Web):** Online banking and emails. Password protected, but normal and safe.
3. **Dark Alleyway (Dark Web):** A hidden part of the internet. You cannot open it with Google Chrome or Safari.

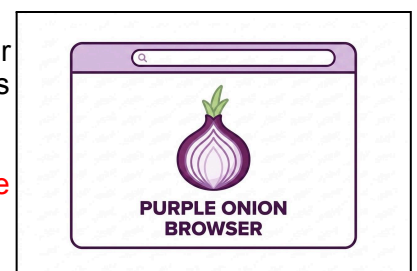
Why is it dangerous? People on the Dark Web are completely anonymous. It is used to share illegal things, bad pictures, and harmful content.



3. How Do Children Access the Dark Web?

Children cannot reach the Dark Web by mistake while searching Google or YouTube. They must download a special browser. The most common one is called Tor Browser.

What to look for: Look on their device for an app icon shaped like a purple onion.



4. Four Simple Rules for Your Home

Use these four simple rules to keep your home safe:



Rule 1: No screens in bedrooms at night

Charge all devices in the living room or kitchen overnight. Children are more likely to search for unsafe content when alone at night.



Rule 2: Lock app downloads

Set devices so children need a password to download new apps.

Use Apple Screen Time or Google Family Link to manage app approvals.

Rule 3: Check for key app icons

Look at their screen regularly for these app icons:

- **Key, Padlock, or Shield:** VPN apps.
- **Purple Onion:** Dark Web browsers.
- **Discord or Reddit:** Social apps where links are shared.

Rule 4: Talk open and calmly

Remind your child regularly:

"If you ever see something online that makes you feel scared, confused, or sad, tell me straight away. You will not be in trouble."

Below is a simple checklist to keep on your fridge or desk.

Child Internet Safety Checklist

Use this quick checklist to review your child's devices.

Step 1: Check App Icons

Look at the main menu or home screen. Check for these icons:

-   **Key, Padlock, or Shield icons (VPNs)**
 - Used to bypass home safety filters.
-  **Purple Onion icon (Tor Browser)**
 - Used to access the Dark Web.
-  **Discord or Reddit apps**
 - Social forums where kids share links.

Step 2: Set Physical Rules

Set simple home boundaries:

-   **Devices stay out of bedrooms at night.**
 - Charge all devices in a shared room overnight.
-  **No screens during mealtimes.**
 - Encourages family interaction.

Step 3: Check Device Settings

Control app access:

-  **App download approvals are turned ON.**
 - On iOS: Use Screen Time passcodes. On Android: Use Google Family Link.
-  **Know device passcodes.**
 - Ensure you can unlock your child's device when needed.

Step 4: Talk to Your Child

Say this to your child regularly:

 **"If you see something online that makes you feel scared or confused, come tell me. You will never be in trouble."**