Paratus Tips

Internet Safety

Beware of Online Scammers

Scammers often pose as friends, teachers, or reputable companies to manipulate children into sharing sensitive information or clicking on malicious links. For example, a scammer might send a message saying, "I'm your classmate and need help unlocking my game – click here!" Children may not realise they are being deceived.

Tip: Teach children to recognise red flags, such as poorly written messages or urgent requests. Use browser extensions to block phishing websites and set up alerts for suspicious links and to validate who they are communicating with via a different channel.

Monitor Gaming and Game Rooms

Online multiplayer games can be fun but often include chatrooms where strangers can directly communicate with children. Some players may engage in inappropriate discussions or attempt to groom young users. Take time to understand the games your children play and encourage gaming with friends they know in real life.

Tip: Disable public chat features or restrict communication to a pre-approved friends list using the game's settings.

Address Cyberbullying Early

Cyberbullying is not always obvious—it can include mean comments, exclusion from group chats, or spreading rumours online. Children might hide their experiences out of embarrassment or fear. For instance, they may be teased in a group chat about their appearance or hobbies. Create an environment where children feel safe sharing their experiences without fear of judgment or punishment.

Tip: Teach children how to block and report bullies on platforms and gaming sites. Encourage them to also raise this with their parents.

Discuss Inappropriate Content and Trends

Social media platforms can expose children to unsuitable memes, explicit videos, or trending topics they might not understand. For example, they might encounter content promoting unsafe or exploitative behaviours.

Tip: Use filtering software to block explicit content on all devices. Review your children's social media feeds together and use these moments to discuss values, boundaries, and context. Consider restricting access to social media at a young age. In some countries, children under 16 are not allowed access to social media.

Manage Screen Time and Wi-Fi Access

Excessive screen time and unrestricted internet access can cause irritability,poor grades, or difficulty sleeping. Apps like TikTok and YouTube are designed to keep users scrolling endlessly, making it difficult to unplug. Monitor signs of digital addiction, such as withdrawal, skipping meals, or avoiding social interaction.

Tip: Establish clear household rules for device use, such as having device-free family dinners and keeping devices out of bedrooms at night. Use your router's settings to manage Wi-Fi access by scheduling downtime during hours like bedtime or study time. Engage children in creating their own screen time goals and consider setting up a guest Wi-Fi network specifically for their devices to ensure better oversight. Use Google Family Link (free) for phones and Microsoft Family Safety (free), to control screentime, content etc.

Protect Against Invasive Ads and Pop-Ups

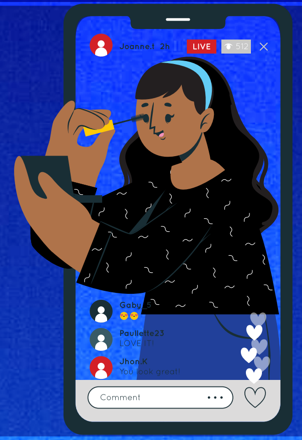
Ad-heavy websites can expose children to scams or inappropriate content. For instance, pop-ups might falsely claim a child has won a prize, prompting them to click on dangerous links.

Tip: Install an ad blocker to minimise exposure to harmful ads. Enable Chrome's built-in "Enhanced Safe Browsing" or on iOS and macOS, enable content blockers like AdGuard or Purify directly through Safari settings.

Understand the Influence of Online Personas

Children are impressionable and often idolise influencers who promote unrealistic lifestyles, unhealthy behaviours, or products requiring parental approval. Beyond reckless challenges, influencers may glamorise excessive materialism, unhealthy body standards, or age-inappropriate trends. They frequently endorse products, like cosmetics or supplements, that may not align with family values or a child's needs.

Tip: Search for and guide your children toward following positive personas, such as conservation experts, educators, doctors, and tech reviewers. This will help them engage with content that inspires learning and growth while encouraging open conversations about values, advertising and responsible decision-making online.



Help Children Recognise Alorithmic Biases

Many apps and platforms use algorithms to personalise content based on user behaviour. This can create "algorithm bias," where users are repeatedly show similar content. For example, a child searching for fitness tips may be inundated with extreme diet culture content. Discuss how algorithms work and how they aim to keep users engaged rather than provide balanced information.

Tip: Teach children to diversify their content consumption, explore varied topics, and always select options to prevent apps from tracking their activity to reduce algorithmic bias and protect their privacy.

Highlight the Importance of Secure Password Practies

Weak passwords are a major cause of data breaches. For instance, using "Roblox123" across accounts could result in multiple profiles being compromised if one account is breached. Teach children to create passwords using random phrases, such as "PurpleHorse$42Sunset."

Tip: Review the child's online user account settings and passwords. Pay attention to D.O.B settings as this can assist with content control when logged in. There are various password managers that can be used safely which generate random and complicated passwords which store those passwords for access in future, making it much more secure.

Teach Consent for Sharing Photos and Information

Sharing photos of friends or personal details online without consent can lead to privacy violations or cyberbullying. For instance, a child might post a group photo without realising one friend did not wish to be included.

Tip: Teach children to always ask for permission before sharing photos or tagging others online. Use privacy settings to manage who can see posts and tagged content.

Set Up Parental Controls on Devices

Parental controls are essential for protecting children online and ensuring a safe and balanced digital experience. Most devices, from smartphones and tablets to gaming consoles and smart TVs, have tools to restrict content and monitor activity.

- Gaming Consoles (e.g., PlayStation & Xbox): Create a family account before your child starts gaming. Use parental controls to manage screen time and restrict games based on age-appropriate ratings.
- Laptops and Tablets: Set up a separate user account with restricted permissions. Enable parental controls to block unsuitable content and limit access to specific apps or websites.
- Smart TVs: Explore built-in parental controls to block inappropriate apps and restrict access to unsuitable streaming content.

Tip: Familiarise yourself with these controls during device setup and customise them to suit your child's needs.

Navigate Deepfake Scams and AI Generated Content

Advancements in AI have made it possible to create convincing fake videos, images, and text that can deceive both adults and children. Scammers may use deepfake content to impersonate trusted individuals, such as teachers or known personalities, to extract information or gain access. AI chatbots can also provide misleading responses if used incorrectly.

Tip: Teach children to question the credibility of AI-generated content and verify requests through another trusted medium, such as directly contacting the individual. Establish clear rules for AI use, encouraging children to involve you when exploring such tools. Show them how to use AI positively and safely, while being mindful of ethical considerations like avoiding plagiarism in schoolwork.

www.paratus.africa/botswana | +267 3912345 | support.bw@paratus.africa

PARATUS

Always Prepared