KPMG

Be cyber smart!

How to keep kids safe online — a parent's guide

KPMG International | kpmg.com/cyberday

The internet is an incredible tool for children to learn, socialize, and have fun. However, with one in three internet users being under 18 years old, the risks associated with online activity are significant and continue to grow. Last year, approximately three out of four children worldwide experienced at least one cyber risk.[1] To help keep your children safe, this guide to internet safety offers valuable tips and advice. As a parent or guardian, protecting your child's online well-being is more important than ever.

[1] The Child Online Safety Index, DQ Institute, 2022.

Talk about online safety early and be a proactive parent

Start talking to your kids about internet safety at a young age. By having these discussions early on, you can help them make smart choices and develop healthy online habits. Educating them about responsible internet use, privacy protection and potential dangers will also protect them from risks. Remember, it's never too early to establish a foundation for safe internet usage.

- **Young people are always eager to learn.** Teach them how to create secure passwords, recognize secure webpages, avoid scams, practice appropriate online behavior and other skills for safe online activity.
- **Don’t give out personal information.** Remind children to never give out personal information, like their full name, home address, passwords or phone numbers, to anyone they don't know.
- **Be careful with strangers.** Talk to kids about the potential dangers of interacting with strangers online and warn them against ever meeting anyone in person without your knowledge and consent.
- **Ask questions.** Be sure to ask your child questions about their online activities, such as what sites they visit and who they communicate with. Encourage them to be open about what they're saying and seeing online.
- **Set clear ground rules.** Moderate screen time by setting boundaries for how long your child is online and what they can do. Screen time unrelated to schoolwork can be made available after homework is complete or on weekends. Keep computers and devices in a common area to oversee all activity.
- **Restrict internet access and monitor activity.** You don't have to be a cyber pro to protect your children online. Parental control apps and those built into devices and Wi-Fi routers are user-friendly. These controls allow you to set access times, monitor internet activity and block website categories. Knowing what your kids are doing online can help to keep them safe. Use this as an opportunity to show your children which websites are appropriate for their age group.
- **Practice what you preach.** Set a good example with your own online presence. Demonstrate safe behavior and practices.

Online gaming? Play it smart!

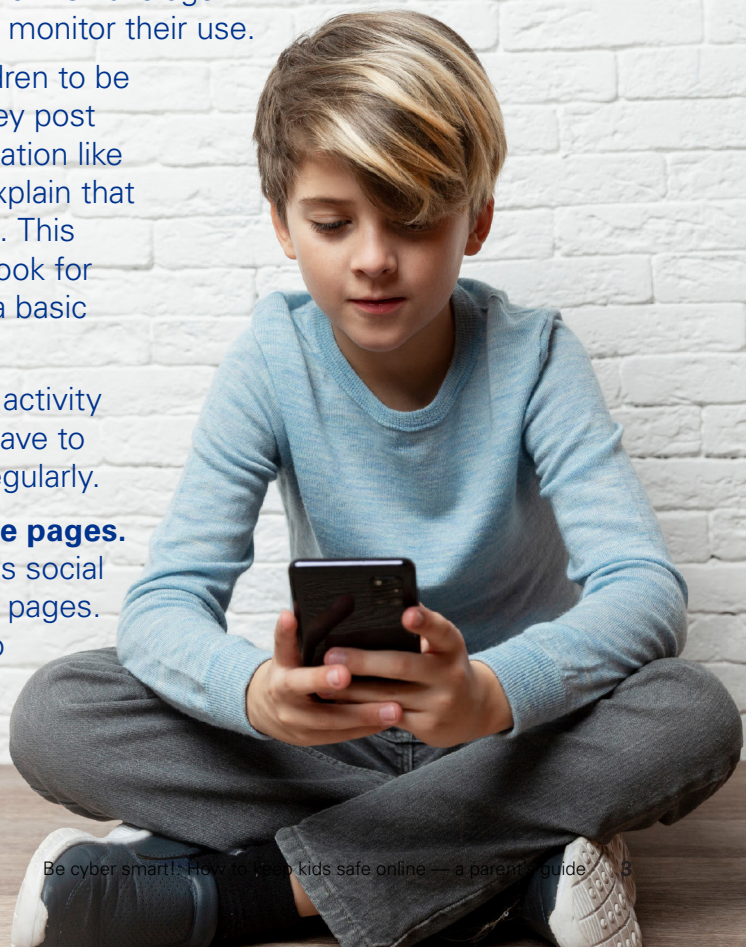
Online gaming can be a fun and social activity, but it also has risks. Cyberbullying, online predators and hidden expenses are some of the concerns that parents should be aware of. To ensure the safety of your kids, here are some tips that you can follow:

- Implement available restrictions to prevent kids from downloading inappropriate apps.
- Set passwords to prevent in-game purchases.
- Establish clear expectations and rules for time limits and the types of games allowed.
- Limit chat conversations to those relevant to the game.
- Ensure your child understands the importance of keeping personal information private and never sharing it online.
- Tell them to report any bullying to an adult immediately.

Social media safety tips

Social media platforms have become an integral part of our daily lives and valuable tools for communication and entertainment. However, there are also significant risks associated with these platforms, especially for children. Kids' misuse of social media can expose them to various dangers, including cyberbullying and online predators. To keep your children safe, here are some tips to keep in mind.

- **Age restrictions.** Most social media platforms have age restrictions. Ensure they are followed and monitor their use.
- **Pause before you post.** Teach your children to be mindful of the comments and pictures they post and stress never to share personal information like their age, school, address or full name. Explain that once it's online, it remains on the internet. This is especially important as kids grow and look for summer jobs — most employers will do a basic online search of potential candidates.
- **Follow your child.** Monitor social media activity by following your child online. You don't have to participate, just view profiles and posts regularly.
- **Review social media parental guidance pages.** To learn more about protecting your child's social media accounts review parental guidance pages. Ensure your child's profile is always set to 'private' mode via account settings and teach them about social privacy settings.



Cyberbullying

Cyberbullying is a type of bullying that involves electronic communication and has unfortunately become more prevalent. While it shares similarities with traditional bullying, cyberbullying can cause even more harm because the aggressor can continue to harass the victim no matter where they go. With the internet and cell phones, anyone can become a cyberbully anytime and from any location. Here's how you can help:

Communicate

It's crucial today to talk to children about cyberbullying. Encourage open communication so they feel comfortable telling you about it. Educate them to:

- Report offensive or hurtful comments immediately, whether they are the target or not.
- Be careful what they say, send, post or blog about others — unintentional bullying is still bullying.

Recognize

Signs of being a cyberbullying victim:

- Showing unexpected anger, depression or frustration after using any device or avoiding device use altogether.
- Uneasiness about going to school or participating in group or team activities.
- Abnormally withdrawing from friends and family members.

Take action

Parents and kids should take action by:

- Saving bullying texts, posts and emails.
- Not replying and not deleting them.
- Reporting the ID online and blocking the user from further interaction.
- Escalating the issue to your child's school or the police as necessary.

Logging in and out securely

Managing multiple passwords can be daunting, especially for kids with trouble remembering them all. However, it's important to recognize that passwords are the primary safeguard against potential privacy breaches that can impact their safety both online and offline. To ensure secure login and logout processes, here are some key tips to help kids protect their personal information better.

Choose usernames wisely

- Avoid using a full name, age, address, date of birth, gender or other personal information.
- Advise children to consult with an adult to create usernames if in doubt.

Practice password safety

- Show kids how to combine phrases, numbers, symbols and uppercase and lowercase letters.
- Stress never to repeat or reuse passwords and to never share a password or provide it if requested.
- Avoid passwords that are easy to guess, such as a birthdate or favorite sport or activity.
- Try using a password manager and suggest to your kids to only remember three passwords: one for school, one for their computer and one for their password manager — with all other passwords being stored there.
- Encourage them to use two-factor authentication where possible.

Protecting your personal information

- Remind your child to always log out when leaving a site or platform.
- Avoid free WI-FI and the risk of data theft by hackers.
- Never share login credentials with others, including friends.
- Advise children to never give out personal information such as their full name, home address, or phone numbers to anyone they don’t know.
- When visiting websites on phones, don't enter usernames and passwords.

Navigating the world of AI safely and securely

As artificial intelligence (AI) programs gain popularity, it's common for children to become curious about them. However, having conversations with kids about responsible and appropriate tech usage is crucial. Consider the following tips to help your family explore and learn about AI together.

How does it work? Explain to your kids how AI technology works so they can appreciate its benefits, understand its potential limitations and learn how to use it effectively. Give them some examples they may already be familiar with to help them comprehend what it is.

How to engage with it. AI tools can help kids be creative and learn new skills. Talk to your kids about AI technology that excites them. Get them thinking about how the programs could help them learn and grow. Encourage them to be critical of the information they get from new technology and to use their creativity to complement AI.

What are the risks? Kids should understand that AI has limitations that can cause inaccurate and biased results. Hackers can also manipulate AI by changing data, which can lead to wrong predictions. Don't forget to remind kids that AI lacks emotional understanding and cannot replace human relationships and connections.

How to use AI safely.

- **Be mindful of personal information.** Kids should avoid sharing sensitive details like their full name, address, phone number or financial information unless they trust the platform and know how they handle personal data.
- **Understand privacy settings.** Take the time to review and adjust privacy settings on AI platforms according to your comfort level.
- **Don’t overshare.** Limit the amount of personal information that is publicly accessible and take note of what data is being collected.
- **Think critically.** Remember that AI systems are not perfect and can make mistakes. Ask kids to check facts, cross-reference information and consider different perspectives before reaching conclusions or making decisions based solely on AI-generated output.
- **Report inappropriate content.** If your child comes across offensive or harmful content or experiences inappropriate interactions, instruct them to report it to the platform, service provider or a trusted adult.
- **Be cautious with AI-generated messages.** If they receive unexpected or suspicious messages from AI-powered accounts or chatbots, don’t share personal information or engage in chats that make them uncomfortable.
- **Don’t solely rely on AI.** Avoid being overly reliant on AI for decision-making. Explain that using AI for schoolwork they didn't create could be considered plagiarism or cheating. Instead, introduce educational AI tools that complement their learning.
- **Stay informed.** Keep up-to-date with the latest advancements and developments in AI technology to better understand AI systems' capabilities, limitations and potential risks. This knowledge will enable your family to make well-informed choices and use AI responsibly.

Six ways to stay on top of your kids' cybersecurity

01

Be involved every day.

To ensure your children's safety online, stay involved and communicate often. Before implementing any safeguards, discuss with your children the reasons behind them so they feel you respect their privacy.

02

Parental controls.

Consider using a parental control tool to manage the increasing number of devices your kids use and to keep them safe online. These tools can help by blocking unwanted web content, restricting the use of risky applications and more. It's important to learn how to use them and keep them updated.

03

Monitor activity.

Review your child's internet activity periodically using your parental control tool to ensure safe practices and habits. Discuss with them which websites are appropriate for their age group and explain why.

04

Manage internet access.

Stay on top of your child's online activity by scheduling internet time to predetermined times, such as after their homework is completed or during the weekend. You can use your parental control tool to limit screen time.

05

Install antivirus tools.

These tools are a powerful line of defense to help protect home computers and devices from viruses and other types of malware that are becoming common. Stress the importance of passwords and personal data safety.

06

Back up your device.

Make sure to back up important information in case of a data failure. For most, that means keeping the original data on the device, a backup on an external hard drive and another on a cloud backup service.

Additional information and resources

To help kids and teens develop safe internet habits, parents can promote safe practices and stay involved. For more resources about safe online habits, please visit kpmg.com/cyberday.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

Designed by Evalueserve.

Publication name: Be cyber smart!

Publication number: 138962-G

Publication date: August 2023