KPMG

Be cyber smart!

A parent guide to keep kids ages 7–10 safe online

Life during the pandemic has certainly been challenging for parents, guardians and children. Like young students of all ages, those in the 7 to 10 age group are turning to their devices every day to learn, play games or interact with their friends. This dramatic increase in screen time is adding another layer of worry for today's busy parents and guardians. Now more than ever, how can parents and guardians help ensure that their children remain safe online?

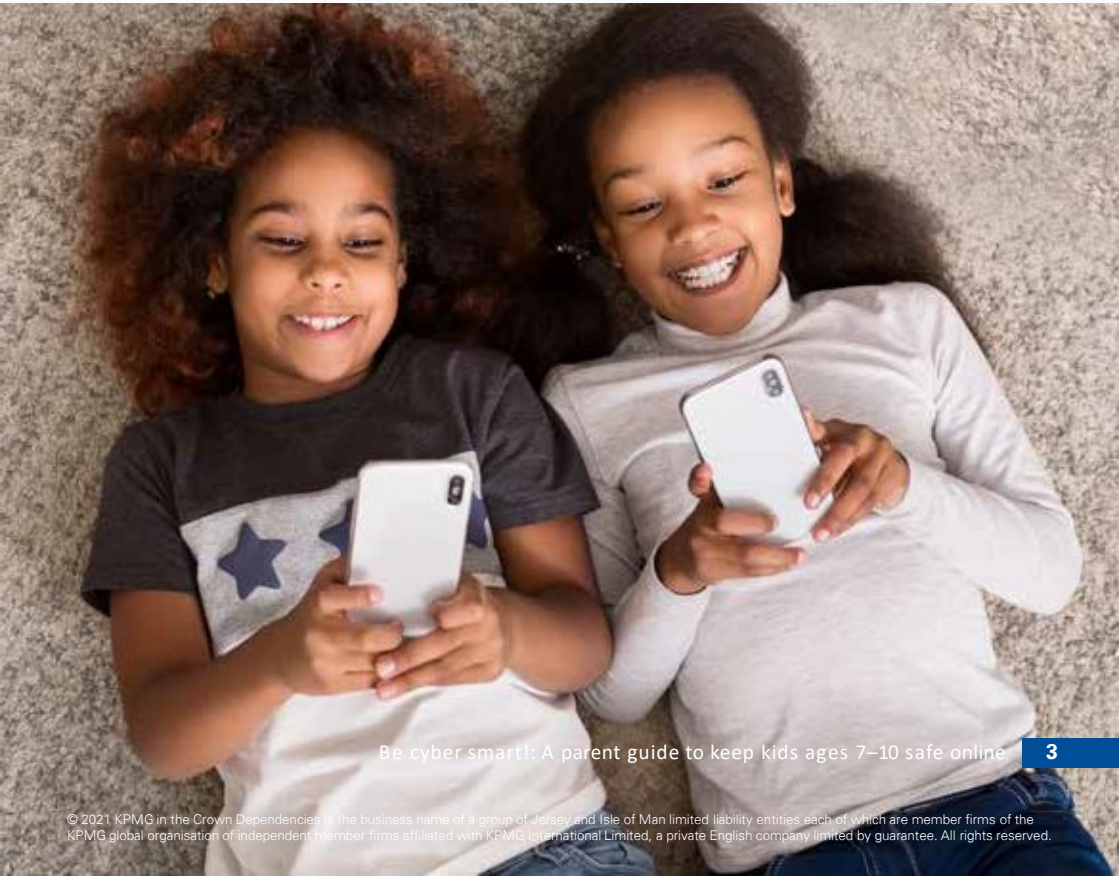
Talk about online safety early and be a proactive parent

The internet is a wonderful resource when used safely. Be open and build trust with your kids, explaining why it's so important to be careful while they're online.

— Young people are always eager to learn. Educate them on using secure passwords, identifying secure webpages, looking out for scams, what appropriate online behavior looks like and other skills for safe online activity.

— Be sure to also ask your child questions about what they do online, such as what sites they visit and who they talk to. Encourage them to be open about what they're saying and seeing while they're online.

— Practice what you preach by setting a good example with your own online presence. Demonstrate safe behavior and practices.



Let's all be cyber smart!

Six helpful tips to keep kids safe online.

1 Set very clear ground rules.
Moderate screen time by setting boundaries for how long your child is online and what they can do. Screen time not related to schoolwork can be made available after homework is finished or on weekends. Keep computers and devices in a common area to oversee all activity.

2 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 easy to use. 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 child which websites are appropriate for their age group.

3 Don't give out personal information.
Remind children to never give out personal information such as their full name, home address, passwords or phone numbers to anyone they don't know. Ensure they create different passwords for every account or use a password manager. A password manager will allow you to store, generate and manage your passwords — minimizing the number of passwords you have to remember. 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.

4 Be careful with strangers.
Talk about the risks of interacting with strangers online and warn against ever meeting anyone in person without your knowledge and consent. Friends only please.

5 Pause before you post.
Teach your children to be mindful of the comments and pictures they post. 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.
Talk to your kids about their social privacy settings and teach them the difference between private and public chats.

6 Be a friend, not a bully.
Talk to your children and educate them to report offensive or hurtful comments to you immediately. If you suspect cyberbullying, encourage open communication so they feel comfortable telling you about it. Also, remind them to be careful about what they say, send, or post about others — unintentional bullying is still wrong. Sharing mean messages empowers bullies and hurts victims even more.

Online gaming? Play it smart!

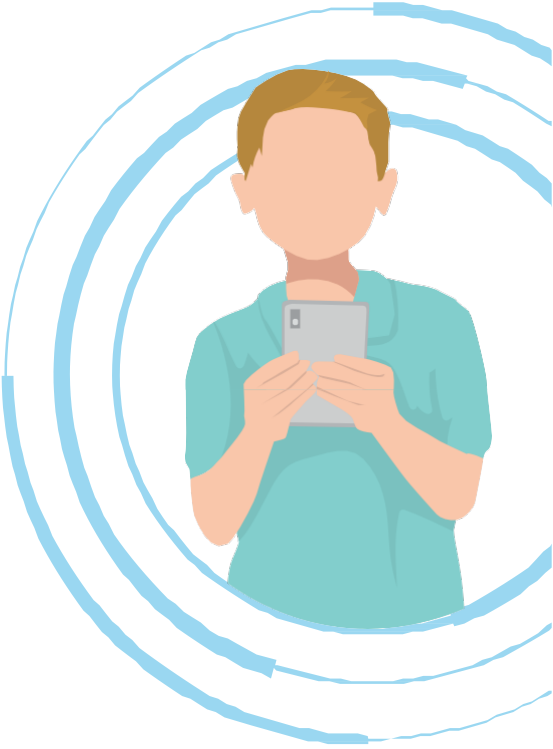
While online gaming can provide hours of entertainment and social connection, there's also a darker side. From cyberbullying to online predators to hidden costs, there are many concerns when it comes to playing video games online, especially for children. Here's how you can help protect your kids:

- Implement available restrictions to prevent children ages 7 to 10 from downloading inappropriate apps.
- Set passwords to prevent in-game purchases.
- Set clear expectations and rules for time limits and allowable games.
- Limit chat conversations to those relevant to the game.
- Ensure your child understands what personal information is and that they should never share it online.
- Tell them to report any bullying to an adult immediately.

Social media safety tips

There are plenty of good things about social media — but also many risks that kids should avoid. From predators to cyberbullies, a child's misuse of a social media can have serious consequences. Here are some tips for keeping your kids safe on social media.

- Most social media platforms have age restrictions. Ensure they are followed and monitor their use.
- Encourage your child to stop and think before posting comments or pictures and stress never to share personal information like their age, school, address or full name.
- 'Friend' or 'follow' your child online to monitor social media activity. You don't have to participate, just view profiles and posts regularly.
- Review social media parental guidance pages to learn more about how to protect your child's social media accounts.
- Data provided to a social network is stored and often shared by default. Ensure your child's profile is always set to 'private' mode via account settings.



Cyberbullying

Cyberbullying is a form of bullying using electronic forms of contact and has become increasingly common. Though similar to regular bullying, cyberbullying takes the trauma one step further by allowing aggressors to follow the victim wherever they go. Virtually anyone, anywhere, anytime can bully another person by simply jumping on the internet or using a cell phone. Here's how you can help:

Communicate

It's crucial today to talk to children openly about cyberbullying. Educate them to:

— Report offensive or hurtful comments to you immediately, whether they are the target or not.

— Be careful what they say, send, post or blog about others — unintentional bullying is still bullying.

Take action

It's important that parents and kids 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.

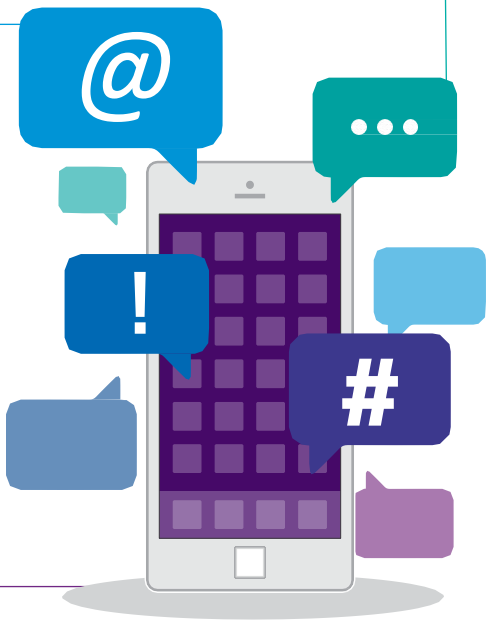
Recognize

Signs of being a cyberbullying victim:

— Showing unexpected anger, depression or frustration after using any device or avoiding device use all together.

— Uneasiness about going to school or participating in group or team activities.

— Abnormally withdrawing from friends and family members.



Logging in and out securely

Keeping track of passwords can be a hassle. Still, passwords remain the first line of defense against an invasion of privacy that can affect safety both on and offline. Here are a few tips that can help kids log in and out securely.

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. Remind your child to always log out when leaving a site or platform.

— It's best to avoid free WI-FI and the risk of data theft by hackers.

— When visiting websites on phones don't enter usernames and passwords.

What can you do? Clear communication is key.

Be involved every day — manage internet access and monitor activity

Being aware, staying involved and maintaining close communication can help keep children safe when using the internet. Innovative control tools built into devices and Wi-Fi routers are easy to use and it pays to become familiar with how they work and how to keep them updated.

Parental controls that protect children from accessing any inappropriate websites can be applied to your network and devices — just be sure to enable them.

Logging and monitoring of your home network lets you review your child's internet activity to ensure safe practices and habits. Discuss with your child which websites are appropriate for their age group and explain why.

Schedule internet time to manage your child's online activity to pre-determined times, such as after their homework is completed or during the weekend.

Antivirus 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.

Back up important information as data gets lost. For anything really important, keep a copy somewhere else, like a USB stick. For anything that needs to survive more than five years, print it out.

Additional information and resources for the 7–10 age group

By encouraging safe practices and staying involved, parents can better educate children in the 7 to 10 age group to develop safe internet habits. The following online resources can be helpful in educating children on how to be safe online and how to always be a cyber friend:

— KPMG Global Cyber Day | home.kpmg/cyberday

— Center for Cyber Safety and Education | www.iamcybersafe.org/s/parents

— National Society for the Prevention of Cruelty to Children | www.nspcc.org.uk/ preventing-abuse/keeping-children-safe/online-safety/

Contact us

Bryan Beesley

Senior Manager, Advisory,
KPMG in the Crown Dependencies
bbeesley@kpmg.co.im

Arthur Mainja

Senior Manager, IT Audit,
KPMG in the Crown Dependencies
amainja@kpmg.com

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

home.kpmg/cds