KPMG

Be cyber smart:

Tips to help keep children safe online

11–16 years old

Life during the pandemic has been difficult for parents and guardians and children alike. Children of all ages, daily now, are turning to their devices for learning, playing games or interaction with friends. This increase in screen time adds another layer of worry for parents and guardians. Now more than ever, how can parents and guardians ensure that their children are being safe online and making sensible decisions?

Talk about online safety early and get involved

— Be honest, open and build trust, explain why it's important to be careful while online.

— Educate them on how to use secure passwords, how to identify secure webpages, how to look out for scams, what appropriate online behavior looks like and many other foundational skills.

— Review your child's internet activity and social media accounts.

— Be sure to also ask your child questions about what they do online, such as what sites they visit and who they talk to.

— Practice what you preach, set a good example with your own online presence.

Be cyber smart

Consider these six tips for keeping your kids safe online.

1. Set some ground rules.

Help moderate screen time by setting boundaries for how long your child can spend online and what they can do. Screen time not related to schoolwork can be restricted to after homework is finished or to weekends. It's also a good idea to keep computers in a common area and monitor your child's activity.

2. Restrict internet access and monitor activity.

You don't have to be a cyber pro to protect your computer and children. Parental control apps and those built into devices, computers, and Wi-Fi routers are easy to use. These controls allow you to set access times, monitor internet activity and block websites categories. Keep an eye on what your kids are doing online will help to keep them safe. Use this as an opportunity to discuss with your child which websites are appropiate for their age group.

3. Don't give out personal information.

Remind your children to never give out personal informarion, such as, full name, home address, passwords, location or telephone number to anyone they don't know online whether through social media or online gaming. To keep their personal information safe, tell them to create different passwords for every online account they have, and then monitor their accounts for elicit activity.

4. Careful with strangers.

Talk about the risks of interacting with strangers whether through social media platforms, discussion boards or online gaming. Instill to never agree to meet anyone outside of the chat. If they want to have an "offline" conversation with this person, they should tell you to arrange a safe way to meet.

5. Pause before you post.

Teach your children to be mindful of what comments and pictures they post online. Explain that once it's online, it will remain on the internet or in cyberspace. This is especially important as kids grow up and are looking for a job; 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/ open chat rooms.

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 they're being cyberbullied, keep communication lines open, so they feel comfortable telling you if they're the target. Also, remind them to be careful about what they say, send, or post about someone else — unintentional bullying is still bullying. Reading or forwarding mean messages empowers bullies and hurts victims even more.

Online gaming

- Determine what games are age-appropriate for your child.
- Ensure your child knows what conversations are acceptable while gaming with strangers.
- Set expectations and rules for time limits and allowed games.
- Ensure your child understands what information is personal and that they should never share that information in-game or online at any time.

Social media

**most social media platforms have age restrictions to create and use accounts. Please ensure you follow age restriction guidelines and monitor any usage.*

- Let your child know to stop and think before they post comments or pictures and never share personal information like age, school, address, or full name.
- 'Friend' or 'follow' your child online so you can check in on their social media activity. You don't have to participate, just view their profiles and posts as often as possible.
- Review social media site's parental guidance pages and work with your child to apply the security settings that best protect their privacy.
- Data provided to a social network is stored and, most of the time, it's shared by default. Ensure your child's profile is set to Private. Go into settings and help them adjust the default controls.

Cyberbullying

Communication

Talk to your child(ren) and 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 someone else — unintentional bullying is still bullying.

Recognition

Signs of being a victim of cyberbullying:

— Unexpected anger, depression, or frustration after using any device or stops using devices all together.

— Uneasy about going to school or participating in team activities.

— Abnormally withdrawn from usual friends and family members.

Action

It is critical to take the right action:

— Save texts/posts/emails.

— Don't reply and don't delete them.

— Report the ID online and block the user from further interaction.

— Escalate to your child's school or the police as necessary.

Remote learning

— Follow your schools remote learning guidelines.

— Prepare your child and create a daily plan.

— Understand the technology and ensure your learning apps are up to date.

— Create school-like environment and set up a dedicated learning space.

— Make sure your child has all the necessary materials to complete assignments.

— Keep your webcam covered when you're not using it.

— Help them find their own motivation.

— Remember to schedule time for fun.

— Mix screen time with old school learning mediums, such as reading from textbooks, making notes.

What can you do?

Restrict internet access and monitor activity

You don't have to be a cyber pro to protect your computer and children. Parental control apps and those built into devices, computers and Wi-Fi routers are easy to use. These controls allow you to set access times, monitor internet activity and block website categories. Keeping an eye on what your kids are doing online will help to keep them safe.

Parental controls can be used to protect your child from accessing inappropriate websites and can be applied to the network as a whole or individual devices.

Scheduled internet time can be used to restrict your child's internet access to pre-determined times such as after homework or on weekends.

Logging and monitoring of your network can allow you to review your child's internet activity to ensure they are using the internet safely. You can also use this as an opportunity to discuss with your child what website are appropriate for their age group.

Antivirus can serve as the last line of defense to protect your computer, and the information stored within, from dangerous viruses and other types of malware.

Additional information

By educating yourself, you can better educate your child(ren) to teach and reinforce good internet habits. The following online resources can be helpful in educating your child(ren) on how to be safe online and how to be a cyber friend, not a cyber bully.

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

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

— Mississippi Dept. of Information Technology Services — Cyber Security for Families — https://www.its.ms.gov/Services/Pages/Security-Links-for-Family.aspx

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name: Be cyber smart: Tips to keep children safe online
Publication number: 137021b-G
Publication date: October 2020