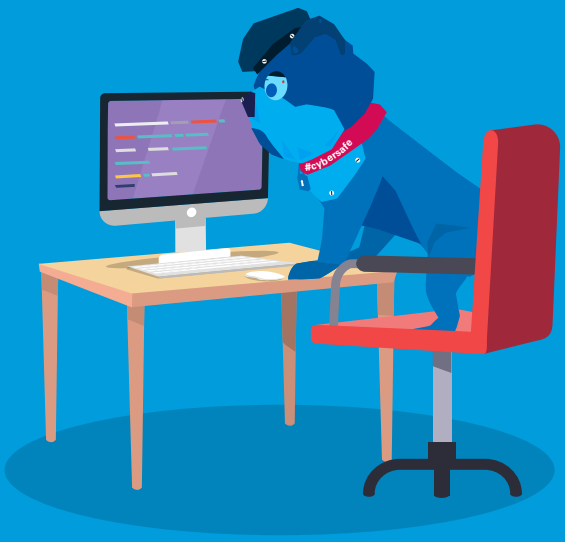
KPMG

Be cyber smart:

Tips to keep children safe online



Talk about online safety and get involved

— Have conversations about online safety. Be honest and build trust, explain why it is important to be careful while online.

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

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

— Ask your child questions about what she/he does online, such as what sites they visit and who they talk to.

Set ground rules and agree on boundaries as a family

— Set boundaries for how long your child can spend online and what they can do.

— Adjust parental controls to suit your child's age and maturity.

— Discuss with your child which websites are appropriate for their age group.

— Communicate what is acceptable online behavior to establish good and bad sharing practices.

— Remind your child that strangers online may not always be who they appear to be.

— Reinforce these boundaries and the need to be skeptical of online strangers.

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 is 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.

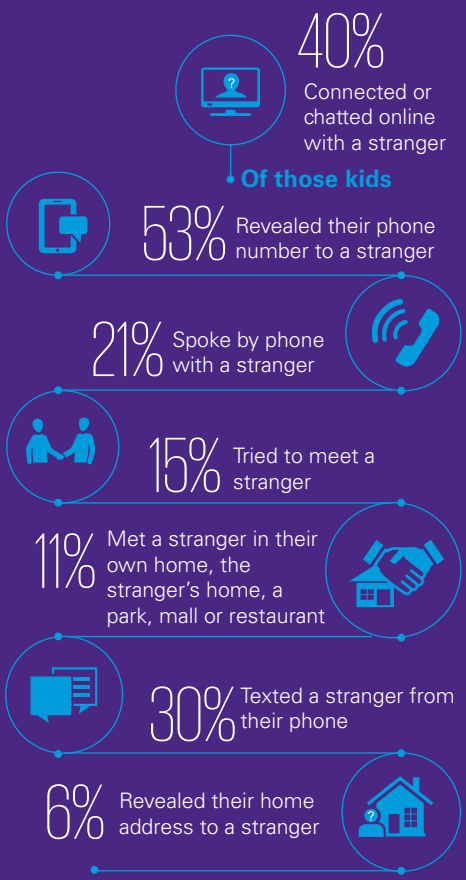
— Don't reply and don't delete them.

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

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

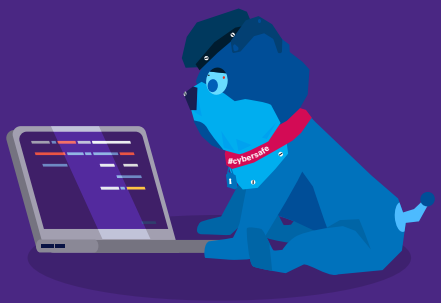
Did you know

Stranger danger



Source: Children's Internet Usage Study conducted by The Center for Cyber Safety and Education

For the complete details of this study, visit www.SafeAndSecureOnline.org/childrens-internet-study/



What can you do?

You don't have to be a cyber pro to protect your computer and network

Many new devices, computers, and Wi-Fi routers come with built-in parental controls that are easy to use, but are often overlooked during the initial setup. These controls allow you to set access times, monitor internet activity and block website categories.

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.

Logging and monitoring of your network can allow you to review your child's internet activity to ensure they are using the internet safely.

Scheduled internet time can be used to restrict your child's internet access to pre-determined times such as after homework and before bed.

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