## Did you know

### Stranger danger



Connected or chatted online with a stranger

Revealed their phone number to a stranger

Of those kids

Met a stranger in their own home, the stranger's home, a park, mall or restaurant 21%

Spoke by phone with a stranger

Texted a stranger

from their phone

Tried to meet a stranger





Revealed their home address to a stranger

### Where kids spend time online



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/ © 2016 Center for Cyber Safety and Education.

### kpmg.com/socialmedia











© 2018 KPMG International Cooperative ("KPMG International"), a Swiss entity, Member firms of the KPMG network of independent firms are affiliated with KPMG International, KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Designed by Evalueserve.

Publication name: Be cyber smart: Tips to keep children safe online Publication number: 135745-G | Publication date: August 2018



# Be cyber smart.

Tips to keep children safe online





## 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.
- Agree as a family so that access to devices can be shared fairly.
- Communicate what are acceptable online posts that respect others.
- Share these rules with babysitters, childminders and other family members.



### Talk about online safety and get involved

- Have conversations about online safety.
- Ask your children questions about what they do online, such as what sites they visit and who they talk to.
- Make the use of the Internet a family activity.



### Use parental and privacy controls

- Check the privacy settings on social media and websites.
- Adjust parental controls to suit your child's age and maturity.
- Remember to always logout of your online accounts.
- 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 and block website categories.
- Don't lie for your child when they want to join a social network, download an app, or purchase a game. Age ratings are in place to help protect your child from inappropriate content.

### Online gaming

— Implement restrictions in the app store to prevent vounger kids from downloading apps above a certain rating and set passwords to prevent accidental in-game purchases.

- Set expectations and rules for time limits and allowed games.
- Limit chat conversations to those relevant to the game.
- Ensure your children understand what information is personal and that they should never share that information in-game or online at any time.

#### Social media

Social media is not inherently bad, and in fact can be a great way for your children to explore the world, express individuality, and connect with friends. There are tips to make sure children use social media safely:

- Let your kids 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 kids so you can check in on their social media activity. You don't have to participate, just take a look as often as possible.
- 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.



### Communication

Talk to your children 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:

- Anger, depression, or frustration after using any devices.
- Stops using devices unexpectedly.

- Stops accessing social media sites, apps, or games.
- 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.

