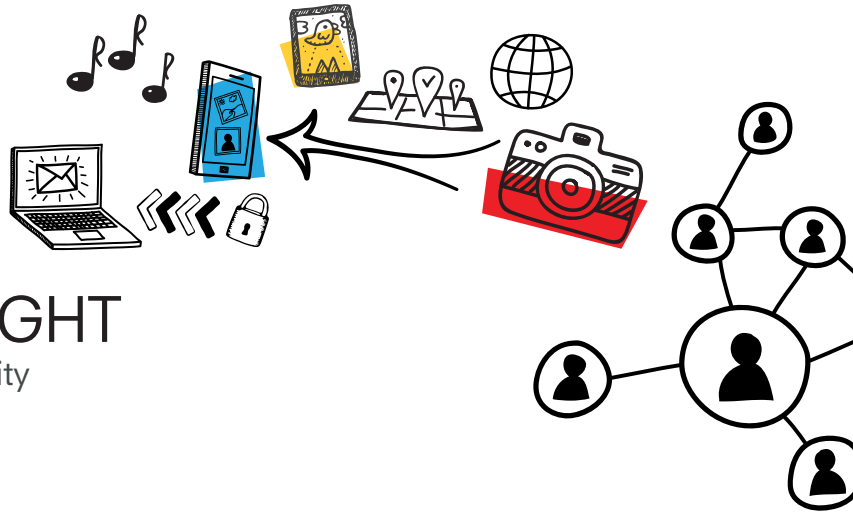# FAMILY
Tech Talk NIGHT
Inspiring Digital Responsibility

Internet Safety **FAQs**

Answers to some of the most frequently asked questions about how to keep your family safe on the Internet.

What can I do to make sure my child is using the Internet safely and responsibly?

- Become familiar with the technology your child uses and the sites your child visits.

- Teach your child that part of being a good digital citizen means treating people with respect, just as she would in person, and notifying an adult when someone is being hurtful or harming others.

- Remind your child that the same digital citizenship rules apply whether he's using the home computer, video game console, laptop, tablet, or mobile phone.

- Use the parental controls or restrictions available in devices, on apps, or on websites to help make sure that your kids are accessing age-appropriate content and that they're using devices, apps, and sites appropriately.

- If you think it's needed, you can consider install-ing Internet monitoring and filtering software. But let your child know in advance that you might be checking in from time to time.

- Tell your child he should personally know everyone on his friends or contacts lists if he uses instant messaging or a social networking site such as Instagram.

- Ask your child to tell you if he sees or receives anything online that makes him uncomfortable. Having an open line of communication is important for keeping children safe online.

- Have ongoing conversations with other parents about Internet safety and responsible Internet use. Discuss your families' rules, ask about theirs, and agree to look out for each other's kids online.
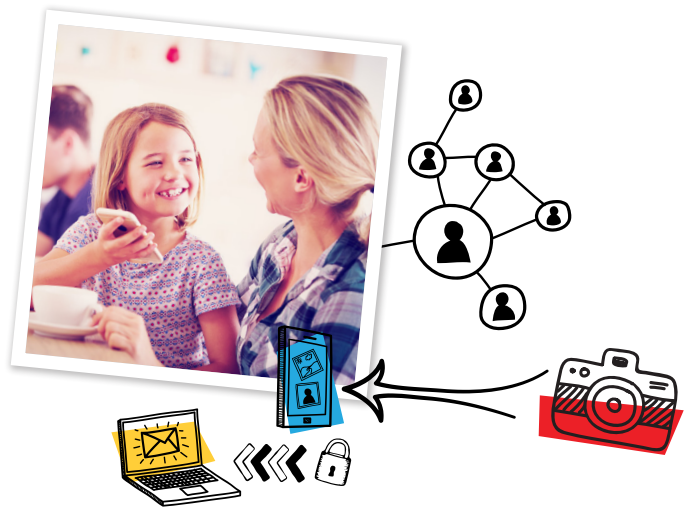
Brought to you by

TREND MICRO™

PTOTODAY
School Family Nights®

FAMILY
Tech Talk NIGHT
Inspiring Digital Responsibility

What should I teach my child about staying safe online?

Even though the risk of being contacted by an online predator is very low, it's still vital that you teach your child the following:

- Not everyone online is who they say they are.

- Never give out identifying information, including your name, address, phone number, and school name.

- Never post public photographs of yourself online or send them to anyone who isn't a close personal friend or a relative.

- Choose a username that doesn't reveal anything about you and is not suggestive or provocative.

- Create strong passwords and keep them secret from your friends.

- Never download or click anything without checking first with a trusted adult.

- Never open an email or accept a social media or gaming friend request from someone you don't know.

- Be wary of "free" offers or promotions. If it seems too good to be true, it usually is.

I'm afraid my child will click on something online that will infect our computer with a virus. How can I keep this from happening?

In addition to making sure your security software is programmed to check regularly for updates, tell your child:

- Never open or forward an email from someone you don't know or click on a link in an email without checking with a parent first.

- Don't use peer-to-peer networks that connect you directly with other users for music downloads or other file-sharing services.

- Never click on a pop-up ad. Use pop-up blockers available through your Web browser.

- Don't download software or apps without permission.

- Be careful when you go to unknown websites for news and information. Just because a search engine displays a link to information you're looking for doesn't mean that site is secure.

## How can I help my child use his cell phone wisely?

- Require a conversation with you or a request for a password before your child can download a new app—and research the app before you approve it. Many apps aren't age-appropriate, are copycats of legitimate apps, or expose users to privacy risks.

- Learn how to use the parental controls that your wireless service provider offers, or consider purchasing security software that allows you to limit calls, texts, and content to and from your child's phone.

- If your child has a smartphone, use the restrictions to limit the types of content (apps, music, TV shows, movies, Internet content) he can access.

- Remind your child that the texts or photos she sends could be shared by others, so she should think before she texts.

- Establish ground rules for cell phone use and the consequences for violating those rules.

- If your child's phone has a camera, make sure your child understands that it's unacceptable to take, send, or even forward inappropriate photos and videos of themselves or anyone else—and in some cases it might even be illegal.

- If your child receives an inappropriate text or image from someone else, advise him to notify

TREND
MICRO

PTOTODAY
School Family Nights®

FAMILY
Tech Talk NIGHT
Inspiring Digital Responsibility
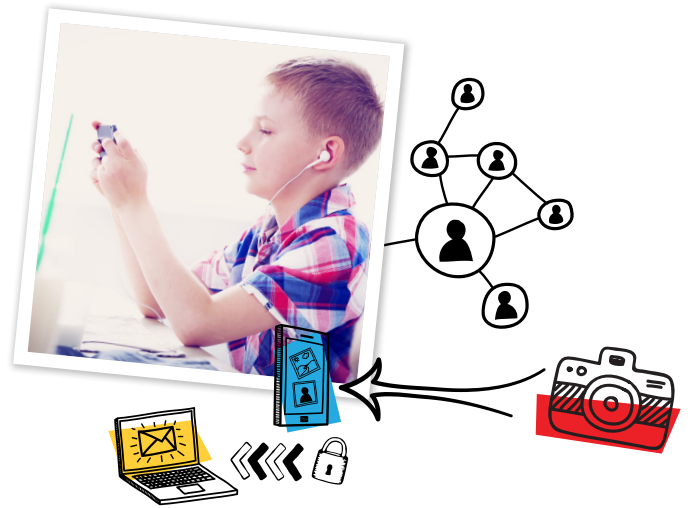
you immediately so you can take appropriate action (such as reporting it to the school or the authorities) and then delete the image.

- Teach your older children who drive that they should never use their phone while driving. Many newer phones can be set up to send an automated text that says "I'm driving, I'll get back to you soon."

- If you have an older child who uses a friend-locator service or app, check his contacts list to make sure only people he knows and trusts are on the list.

- Consider turning off the GPS feature for the camera and certain apps. You will need this location service feature for some apps (such as Google Maps or Waze) but not for others (such as the camera or many games).

- Have your children charge their phones outside of their bedrooms at night, ideally in a common area like the kitchen or family room where parents are able to see all devices.

- Talk about balance and good time management with smartphones and other devices, and model those good habits. Remind your child to stay in control of the device and not to let it control him.

At what age is a child ready to have a social networking profile?

Most social networks require users to be at least 13 years old (though there are some designed for those under 13, with lots of parent oversight). There is no real way to police this activity, however, and surveys have indicated that millions of kids younger than 13 have a social networking profile. Consider your child's maturity level before allowing him to join an online community, and then teach him to follow the rules of the community. To help your child safely navigate social networks, consider these options:

- Find a social networking site suitable for your child's age and maturity level. You can read reviews of sites on **www.commonsensemedia.org**. Under "Apps & Games," click "Website Reviews."

- If your child creates an account on a social networking site, create your own account and "friend" your child so you can keep tabs. It's also a good idea to ask your child for his password so you can check up on his activity.

- If you're not comfortable "friending" your child, consider using social network monitoring products or services. Be sure to tell your child that you will be monitoring him. Open and ongoing communication is key; you want your child to feel comfortable coming to you at any time if something goes wrong.

- Help your child set the privacy controls so his information is visible only to people he has accepted as online friends. ConnectSafely has published parents' guides to several social media platforms. They are available at **www.connectsafely.org**.

- Remind your child not to post anything she wouldn't want others to find out. Even within a trusted circle of friends, someone could take a comment or photo and distribute it to others.

What should I know about cyberbullying?

Cyberbullying doesn't happen to everyone, but it can occur among children of any age who use the Internet, particularly on social media and in the gaming world. It can be devastating to a child because online bullies often feel emboldened by the anonymity of the Internet to say and do things they wouldn't in person. Cruel and hurtful comments can also spread quickly among classmates through the Internet and reach children at home, giving them no refuge from the harassment.
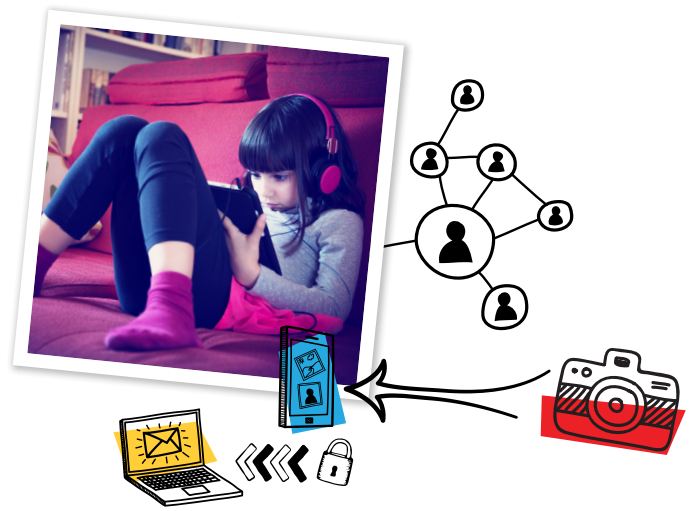
Brought to you by

TREND MICRO

PTO TODAY
School Family Nights®

FAMILY
Tech Talk NIGHT
Inspiring Digital Responsibility

When talking with your child about cyberbullying, emphasize the following:

- Be respectful of others online. Don't post anything you wouldn't want posted about yourself. Also, you're more likely to be bullied online when you post mean or hurtful posts about others.

- Don't participate in online bullying, either directly, by retaliating, or by forwarding hurtful posts.

- Don't be a bystander—tell a parent, teacher, or someone else you trust if you're being bullied or you see another person being bullied.

- Save the offending posts in case they're needed to take action against the bully.

- Most Internet service providers, websites, apps, and cell phone companies also have policies against harassment. Reporting an incident on a site or within an app can result in the bully's account being revoked.

If the bullying persists and it's among kids who attend the same school, the first step should be to report it to the school. Many schools are legally required to have processes and policies in place that must be followed to investigate and mediate any bullying that affects its students.

Also, check to see whether your state has a cyberbullying law. Call your state attorney general's office or go online and search your state's name and the words "cyberbully law."

Visit **https://internetsafety.trendmicro.com** for more information. We also recommend "A Parent's Guide to Cyberbullying" at **www.connectsafely.org**. And the Cyberbullying Research Center provides an excellent resource at **https://cyberbullying.org/report**. It's a frequently updated list of contact information for social media apps, gaming networks, and related companies—so you can find exactly where and how to report cyberbullying behavior.

How can I best work with my child's school?

Technology and going online are part of schools' curricula. But since schools are not strictly mandated to share information about Web-based assignments ahead of time, it's up to you to establish communication with teachers and administrators. Remember, they're an important part of the ongoing conversation about Internet safety.

Here are some questions to ask your child's teacher:

- Do you speak to the class as a group about using the Internet wisely and being good digital citizens?

- What types of sites will my child be directed to? Keep in mind, this can vary widely depending on your kids' ages. For example, there's a big difference between learning sites designed specifically for children and news sites like CNN.com.

- What's the best way to keep in touch about these issues? Some teachers might be willing to let you know ahead of time when your child gets an Internet-based assignment, but most will probably find it easier to respond to an email from you. Be willing to communicate in whatever way works best.

- What do I do (and who should I contact) if my child tells me about cyberbulling or unkind behavior online or among classmates? (Teachers definitely want to know about this, so a first step is to approach them. From there they can provide support like connecting parents with the principal, guidance counselor, and each other, if needed.)

Brought to you by

TREND MICRO™

PTO TODAY
School Family Nights®