FAMILY TECH TALK
Virtual Edition

Inspiring Digital Responsibility

Internet Safety **FAQs**

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

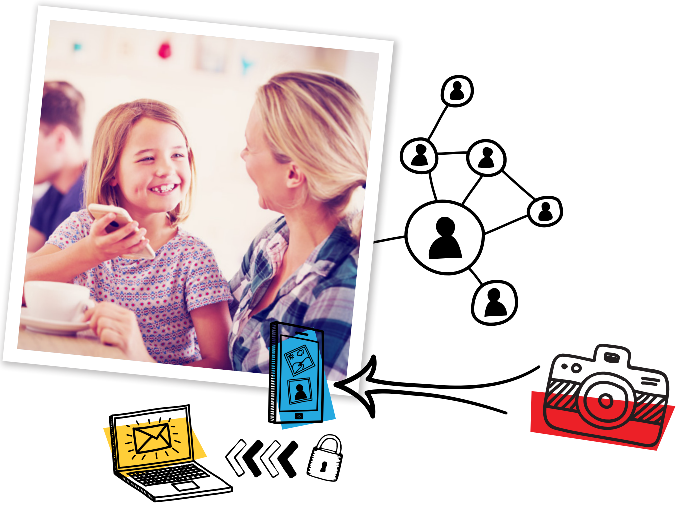
- Become familiar with the technology your child uses and the sites your child visits.
- Teach your child that part of being a good digital citizen means treating people with respect, just as she would in person, and notifying an adult when someone is being hurtful or harming others.
- Remind your child that the same digital citizenship rules apply whether he's using the home computer, video game console, laptop, tablet, or mobile phone.
- Use the family settings or parental controls 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 installing 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™ PTO TODAY School Family Nights®

FAMILY TECH TALK
Virtual Edition

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.

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

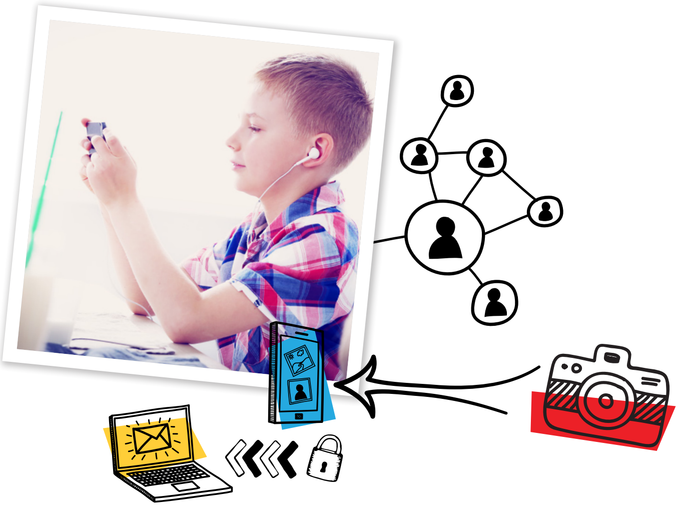
Most social networks require users to be at least 13 years old (though there are some designed for those under 13, with lots of parent oversight). There is no real way to police this activity, however, and surveys have indicated that millions of kids younger than 13 have a social networking profile. 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.

Brought to you by

TREND MICRO™

PTO TODAY School Family Nights®



- 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.

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.

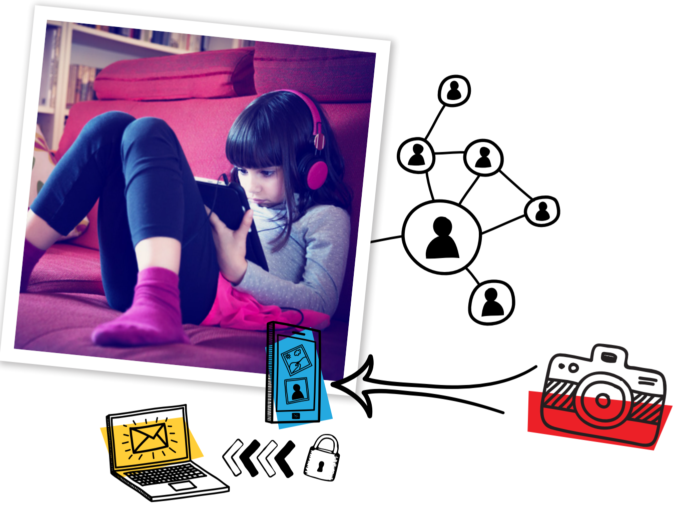
Also, check to see whether your state has a cyberbullying law. Call your state attorney general's office or go online and search your state's name and the words "cyberbully law."

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 do I protect my family's personal information and security now that my children videochat every day for school and to talk to their friends?

- Choose a videochat app that has end-to-end encryption to keep it more secure, and always download any updates as soon as they become available.
- Use a strong password and change it often. Remind your child that you never share passwords.

FAMILY TECH TALK
Virtual Edition
Inspiring Digital Responsibility



- Review and use the app's privacy settings, and teach your child to invite only people they know to chat.
- Encourage your kids to limit invitations and to ask everyone in the chat before inviting others to join.
- If possible, require a password to join a chat or set up a waiting room so you can approve attendees. Lock your child's chats to prevent outsiders from joining.
- Teach your child never to share personal or private information during a chat—no one knows who might be listening on the other end.
- Respect the privacy of the other people in the chat; have your child wear headphones to keep their information private from your family.
- If possible, turn off location tracking within the app.
- If a stranger tries to contact your child through the app, call local law enforcement and the National Center for Missing and Exploited Children at 1-800-THE-LOST.
- For more information, watch our "Protect Your Family on Videochat Apps" webinar at **https://internetsafety.trendmicro.com/webinars/protect-your-family-on-videochat-apps**.

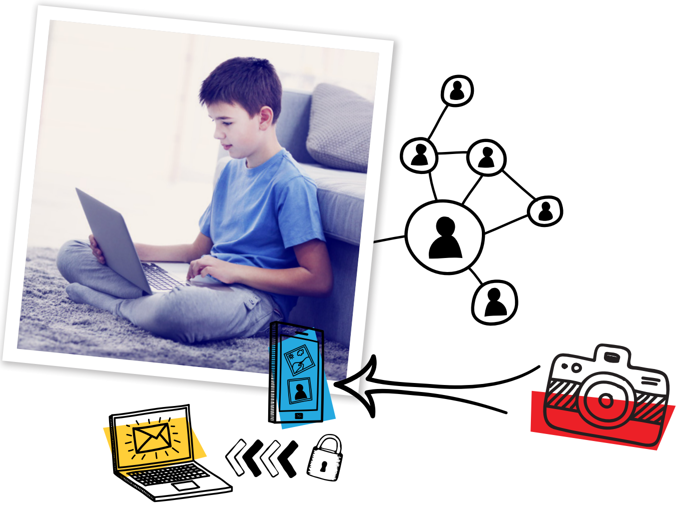
What do I need to teach my child about privacy online?

Every time your child opens an app, plays with a smart toy, posts on social media, or videochats with friends, it's an opportunity to teach them to safeguard their (and your) privacy.

- Teach your child to check the URL of a website and look for the S in "https"—it stands for "secure." Those should be the only sites your child visits.
- Set a password for everything with a unique, complex set of letters, numbers, and symbols. Remind kids that you never share passwords.
- Use privacy settings, add only required information, and click "opt out" whenever possible to limit how much of their personal information is shared. Third-party apps, like a quiz in Facebook, for example, take personal information from your child's profile so limit personal information to only what's required.
- Talk to kids about keeping private things private. Information can be shared and last for a long time, so talk to them about not posting explicit photos, an overly revealing rant, or anything else that might get them into trouble. Give them guidelines they can use to talk with their friends about respecting each other's privacy.
- Turn off location sharing on your child's devices, both in the phone setting and in the apps they use, so their location isn't automatically tagged. Make sure your kids never tell strangers their address, their school name, where they hang out, or where they're going to be. Teach your kids to choose "no" when asked to share their locations.
- Coach your child to respect others and their privacy. They should never record or stream a videochat and share it elsewhere, especially without the other person's consent. That's a big violation of privacy.
- On videochats, let your child know that if others have chosen to hide the video image or use a background, your child needs to respect their decision and never bully someone because of their choice.
- Privacy works both ways. Have kids use headphones to keep other people's personal things private from other family members.

Brought to you by

TREND MICRO™ PTO TODAY School Family Nights®



- If you use a home assistant like Amazon Alexa or Google Assistant, set some ground rules for how your kids can use the device. Set your device so the microphone is turned off when no one's using it. You can also check your device's app settings to delete info you don't want stored.

I've allowed my child to spend more time playing videogames lately because it's a way he can keep connected with his friends. How do I keep him safe on gaming apps?

Almost all videogames today allow players to chat with and compete against family, friends, or strangers from anywhere in the world, in real time. Protect your child while they're gaming with others in the following ways:

- Play the game with them once or twice to understand how the social parts work and how you can control access.
- Identify where in your home your kids can play so you can easily check on them.
- Set limits for family, privacy, and social aspects of the game to limit who they can interact with.
- Learn more about the chat function. Find out whether chats are scripted or free form and how you can restrict or limit them.
- Remind your child about using kind behavior online.
- Encourage them to come to you if they experience anything scary or troubling, and report suspicious users to the app or game, if possible.
- If the behavior they report is extremely disturbing, such as grooming behavior from someone your child doesn't know, consider contacting the National Center for Missing and Exploited Children at 1-800-THE-LOST.

How do I keep my child from using a fake game app?

Cybercriminals are constantly creating gaming applications that look legitimate but actually put your personal information at risk. Some fake apps sell "cheat codes," lock your child out of a game until you pay a ransom, and more. Here's how to help keep your kids from falling prey to phony games:

- Research games and choose only those that have a good reputation and are used by a lot of people.
- Use up-to-date security software on your devices to prevent clicking on harmful downloads.
- With more complex games like Fortnite or Apex Legends, teach your child not to buy "cheat codes" (like aimbots or wallhacks) to defeat another player or win the game. Not only could your child get kicked out of the game for cheating; buying those codes could also put your personal data (like credit card information) at risk.