



Internet Safety FAQs



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

How do I teach my kids to be safe and responsible online?

First, you need to understand the world they live in. It is easier to teach a child to do something well if you are able first to do it yourself. Become familiar with the sites, applications, and technologies they use. You don't need to become a frequent user of Facebook or Twitter to understand how it works (and it doesn't take a master's degree to learn it). Just spend some time understanding how to set up profiles or review the content of websites they want to use. The best way to teach your kids about the safe, responsible use of the Internet is by being engaged yourself in the technology your kids do and will use.

Second, it's important to know what the risks are. While even one incident is too many, the likelihood that your child will be contacted by a sexual predator online is very slim. Research shows that the children who are most vulnerable online are those who are likely to engage in risky behavior in other areas of their life. There are greater potential risks of things like bullying or sharing too much personal information.

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 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.

- Never download or click anything without checking first with a trusted adult.
- Never open an email from someone you don't know.
- Be wary of "free" offers or promotions. If it seems too good to be true, it usually is.

What else 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 being a good digital citizen means treating people with respect, just as you would in person, and notifying an adult when someone is being hurtful or harming others.
- Keep the computer in a common area of your home where the monitor will be visible to others.
- Use the parental controls in your Internet browser or security software. Most have parental controls that allow you to block websites by categories or even by age.
- Consider installing Internet monitoring and filtering software.
- Make sure your child personally knows everyone on his friend or contact lists if he uses instant messaging or a social networking site such as Facebook or MySpace. Sit down with your child and ask him to identify each name on the list.
- 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.

Sponsored by



Presented by





Internet Safety FAQs



What if my child accidentally views or reads inappropriate content?

- Make sure your child knows to turn off the monitor and to tell you or another trusted adult right away.
- Reassure him that it wasn't his fault.
- Use the opportunity to talk about your own family's values.

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 to others an email from someone you don't know.
- Never 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 from a website that you don't know and trust.
- Go only to trusted 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 keep my child safe while playing online games?

- Learn what your child is doing by playing the games with your child and other players.
- Set the parental controls in the gaming console.

- Keep the gaming console in a common area of your home so you can easily monitor the action.
- Become familiar with the privacy and security policies of online gaming services (such as Xbox 360) and decline or block any type of information-sharing that is available through the service.
- Make sure your child knows not to give out identifying information if he is communicating with other players online.
- Establish rules about the games your child may play and whom he may play with.

How can I make sure my child doesn't use his cell phone inappropriately?

- Learn how to use the parental controls that your wireless service provider offers or consider purchasing security software that allows you to control calls, texts, and content to and from your child's phone.
- If you have an older child who uses a friend-locator service or app, check his contact list to make sure only people he knows and trusts are on his contact list.
- Establish ground rules for cell phone use and consequences for violating them.
- If your child's phone has a camera, make sure your child understands that it's unacceptable to take (or send) inappropriate photos and videos—and in some cases, sending them may be against the law.
- If your child receives an inappropriate text or image from someone else, advise him to notify you immediately so you can take appropriate action (such as reporting it to the school or the authorities), and then delete the image.

Sponsored by



Presented by





Internet Safety FAQs



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

In 2011, 7.5 million kids younger than 13 in the United States had a Facebook profile, according to Consumer Reports. The most popular social networks, Facebook and MySpace, have policies forbidding children younger than 13 from using their sites, but because there's no way to enforce the restriction, many children lie about their age to create an account.

- Find a social networking site suitable for your child's age and maturity level. You can read reviews of many websites on www.common sense media.org. Under "Reviews," click "Websites."
- 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. It's important 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. A good reference for setting Facebook controls is "A Parent's Guide to Facebook" from 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 is most common among middle-school-age children, but it can occur among children of any age. 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 trusted adult if you're being bullied or you see another person being bullied. By doing nothing, you send the message that bullying is OK.
- Save the offending posts in case they're needed to take action against the bully.

If the bullying persists, you might want to look into filing a complaint against the bully. Most Internet service providers, websites, and cell phone companies have policies against harassment. You may be able to have the bully's account revoked. 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." If the bullying is occurring among kids who attend the same school, report it to the school. More schools now have processes and policies in place that the school must follow to investigate and mediate any bullying that affects its students.

For more information on cyberbullying, read the "Cyberbullying FAQs" handout that you received during Internet Safety Night, or visit www.trendmicro.com/internetsafety. We also recommend the Tips To Help Stop Cyberbullying from ConnectSafely.org (www.connectsafely.org/Safety-Tips/tips-to-help-stop-cyberbullying.html).

Sponsored by



Presented by

