INTERNET SAFETY NIGHT

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 technological world they live in. It is easier to teach a child to do something well if you are able to do it yourself. Become familiar with the sites, applications, and technologies your children use. You don't need to become a frequent user of Facebook or Twitter to understand how it works. Just spend some time learning how to set up social media profiles or review the content of websites they want to use. However, the explosive growth of social media sites and mobile Internet access makes it impossible for parents to keep up with everything their children do online. Therefore, it is essential that you communicate to your kids your values around online interactions, and your expectations for their safe and appropriate use of digital media.

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 behaviors 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 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 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.
- Make sure your child accesses the Internet from common rooms in your home, whatever device he is using, and don't allow him to go online behind a closed door.
- Remind your child that the same digital citizenship rules apply whether he is using the home computer, video game console, laptop, tablet, or mobile phone.
- Use the parental controls in your Internet browser or security software. Most have parental controls that allow you to block websites by category or even by age.
- Consider installing Internet monitoring and filtering software.
- 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 Facebook.

INTERNET SAFETY NIGHT

Internet Safety FAQs

- 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.

What if my child accidentally views or reads inappropriate content?

- Make sure your child knows to turn off the screen 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.
- Consider installing filters on any Internet-connected devices so it doesn't happen again.

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 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 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 or mobile device to limit the games your child can play.
- 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 or Wii) and decline or block any type of information-sharing that is available through the service.
- Make sure your child knows not to give out personal information if he is communicating with unknown players online.
- Establish rules about the games your child may play and with whom he may play.
- Consider whether you want them playing against people they don't know through online communities such as Xbox Live. If not, you can turn off this feature on the gaming console.

How can I make sure my child uses his cell phone wisely?

- 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 parental controls to limit the types of content (apps, music, TV shows, movies, Internet content) your child can access.
- Remind your child that the texts or photos she sends could be shared by others, so think before you text.
- Establish ground rules for cell phone use and the consequences for violating those rules.

INTERNET SAFETY NIGHT

Internet Safety FAQs

- 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, 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.
- Teach your older children who also drive that they should never use their phone while driving.
- 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) but not for others (such as the camera or many games).

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, including 5 million kids younger than 10, according to Consumer Reports. And this is the case even though Facebook has a policy that forbids children younger than 13 from using its site. But because there is no real way to police this activity, the under-13 crowd keeps growing, oftentimes with parents' permission.

Most social networks require you to be at least 13 years old, though there are some designed for those under 13 (with lots of parent involvement). 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 "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. 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 does not happen to everyone, 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.

INTERNET SAFETY NIGHT

Internet Safety FAQs

- 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. 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. Many schools are legally required to have processes and policies in place that the school must follow to investigate and mediate any bullying that affects its students.

For more information, 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 at **www.connectsafely.org**.