Ten Tips to Keep Kids Safe Online

Marian Merritt

<http://us.norton.com/kids-safe/article>



The task of protecting our children online is a challenge that grows in complexity every day. Just a few years ago, parents mostly worried about the risks of "stranger danger" and online predators. Recently, research from the Harvard University-based [Berkman Center](http://cyber.law.harvard.edu/research/isttf) downgraded online predators to a much lower risk category, but we still have many online risks to educate our children about. These risks can be categorized into three groups.

**Cybercrime**

The first category is cybercrime--or the threats caused by **financially motivated strangers**. Whether in the form of [computer viruses](http://us.norton.com/security_response/index.jsp), [Trojan horses](http://us.norton.com/security-glossary/article), [phishing](http://us.norton.com/security_response/phishing.jsp) attacks, or [spam emails](http://us.norton.com/security_response/spam.jsp), [cybercrime](http://us.norton.com/cybercrime/) keeps growing and changing each year. It's so important for parents to stay on top of the varied threats. This can be daunting, especially if you feel you aren't tech savvy or don't know where to look for help. Fortunately there are several steps you can take to keep cybercrime in all its forms away from your computer, your home network, and your family's information. Follow these tips yourself, and pass them along to your kids.

* **Use an Internet security suite**, like [Norton 360](http://us.norton.com/360/) or [Norton Internet Security](http://us.norton.com/internet-security/), on all computers you own. Using plain antivirus is just not enough protection. You need a full [firewall](http://us.norton.com/360/), antispyware, and other protection a suite can provide.
* **Keep your home network secured** with a good password and security settings.
* **Learn to avoid clicking links**, responding to ads, and opening emails when they come from someone you don't know or appear suspicious. Just take that extra moment to call your friend ("Did you post that link?"), type the URL for your bank, or otherwise display your worldly wisdom by **not** falling for these social engineering tricks.
* **Use a good password** (unique and complex) on all accounts and devices. The two most important account passwords are for your social network and your email account. If a hacker gets control of your social network, he can scam your friends. If he has your email, he can reset the password on all your other accounts by using the ubiquitous "forgot my password" link.
* **Talk to your kids about avoiding cybercrime**. They need to be just as cautious as you. It's also important that they know if they can talk to you when they make an online mistake, like falling for a scamware alert and downloading something dangerous to the computer. Many kids are savvy enough to realize when they've downloaded a virus, but few are comfortable admitting their mistake to their parents.

**Cyberbullying**

The second category is the harm that can befall your child from **people they know.** Typically, this means cyberbullying, the single most common online harm our children will experience. Statistics vary, but at least 20 percent of kids will receive harassing, hateful, or insulting messages via social networks, emails, instant messages, videos, and texts.

Interestingly enough, unlike its non-tech relative, cyberbullying inherently allows roles to be reversed almost instantaneously. The victim can become the bully just by responding to a mean email with another verbal volley.

We have much work to do in our schools and online communities to promote online civility and kindness. We also need to promote appropriate responses when a child is confronted with cyberbullying. A great resource for information about all forms of bullying can be found at <http://www.stopbullying.gov/> and specifically about cyberbullying at <http://www.cyberbullying.us/>

* **Advise your kids never to share passwords**, not even with a close friend. If they think they did, they should change the password.
* **Teach your children to log out of computers** when they finish their work, even at home. This will prevent a friend or sibling from posting or emailing using their account--even as a joke.
* If your child is being cyberbullied, teach them to not respond, to keep a copy of all the messages, and to report it to the school or website. If the messages include threats, report this to the police. If you report the cyberbullying to the school, be sure to follow up in person and ask for a written plan on how the school will respond to the problem. Most states have laws against this form of abuse, and schools have an obligation to address the issue when made aware of it.

**Online Reputation**

The third category of online risk is the harm **we cause ourselves**. This can take many forms, including sexting (sending sexual content by photo, video, or text message); posting information or images of a private, embarrassing, or controversial nature; and even neglecting to set privacy settings.

Sexting is definitely not something we want our underage kids to engage in. Child pornography and other laws may require teachers, parents, and law enforcement to get involved if they become aware of these messages. Kids may think they are sharing these images within a private relationship, but too often the recipient shares the images, for any number of reasons. Perhaps the relationship has ended, maybe the recipient is bragging to friends, or perhaps a friend saw the images on the phone and forwarded them to others. (That is another reason to put a password on all devices!)

"[Online reputation](http://us.norton.com/yoursecurityresource/detail.jsp?aid=online_reputation)" is a term for all the information available about you on the Internet, whether through conducting a search or by viewing your profile on a social network. That composite portrayal of you can serve as a digital dossier, telling a story that may distort the real facts of who you are. We've often heard of young people self-sabotaging their academic, career, and romantic futures with silly posts, photos of underage drinking, or membership in controversial online groups.

The issue of privacy on the Internet is a growing concern for many. We each need to take steps to keep our personal information protected by securing our online accounts, limiting the information we post in public forums, and opting out of unused or unwanted online services. Our lives are being publicly documented to a degree that is increasingly uncomfortable. Just do an online search of yourself and you'll see your 10K race scores, your home's mortgage information, and your tagged photos on your social network. Private information can be used in numerous annoying and harmful ways, so it is increasingly worthwhile to pay attention to privacy issues--and to pass along good advice and habits to your kids.

* **Use the security and privacy settings** on your social network and all accounts to limit who can access your posts.
* **Learn about parental control settings** for your phones, gaming devices, tablets, and all computers. A great tool is the free [Norton Family](https://onlinefamily.norton.com/familysafety/loginStart.fs) for PCs and Macs.
* **Talk to your kids regularly about how to use technology.** Set rules and limits, and keep technology out in the open. Learn about "[The Talk](http://us.norton.com/the-talk/article)," and make it an annual discussion, or for whenever you introduce new technology into your family life.