

# KEEPING YOUR CHILD SAFE ONLINE

DAUPHIN COUNTY MH/ID PROGRAM  
OCTOBER 2018 RESOURCE SHARING

October is National Cyber Security Awareness Month. Our information technology department recently passed along the links below from the Department of Homeland Security. They provide information and resources for keeping your children “cyber safe”. Most youth today have some sort of mobile device, smart phone, tablet or laptop. Although these devices can help children with their schoolwork and stay in touch with family and friends, there are risks associated with using them. However, there are some simple steps that can help can your children stay safe while using their devices and getting online.

I have pulled out a “Top Ten” list from the sites below, but please spend a few minutes visiting them yourself for much more detailed information and ideas.

## **Basic phone/computer tips to help keep your child safe:**

- 1. The phone should default to a locked setting.** The only people who should have that access code are the child and parent.
- 2. Parents should know every password to every device and every password to every app on that device.**
- 3. Check those accounts—as well as messaging programs and texts—for disturbing content on a regular basis.**
- 4. Make sure your child is using appropriate screen names that won't encourage predators.**
- 5. Check the privacy and security settings on the phone and the apps and make sure they are up-to-date.**
- 6. Learn about how photos are “geotagged”.** Your photos could be tagged with your child's exact location. You should be able to turn this feature off in settings.
- 7. Teach your children to never respond to calls, texts or emails from unknown numbers or people.**
- 8. Talk early and often to your child about the dangers they may find on the other end of the line.** Be open and honest. If your child does encounter a bully or other disturbing content, you want him to feel like he can come to you for help.
- 9. Talk to you child about what constitutes appropriate language and photos.**
- 10. Teach your child to program the privacy settings on social media feeds to the highest level and to reject and “friend requests” from those they don't know and trust.**

[Keeping Children Safe Online](https://www.us-cert.gov/ncas/tips/ST05-002) <https://www.us-cert.gov/ncas/tips/ST05-002>

[Rethink Cyber Safety Rules and the “Tech Talk” with Your Teens](https://stopthinkconnect.org/resources/) <https://stopthinkconnect.org/resources/>

[Stop.Think.Connect. Toolkit](https://www.dhs.gov/stopthinkconnect-toolkit) <https://www.dhs.gov/stopthinkconnect-toolkit>

[Stay Safe Online](https://staysafeonline.org/) <https://staysafeonline.org/>

[Concerned Parent's Internet Safety Toolbox](http://backgroundchecks.org/the-concerned-parents-toolbox) <http://backgroundchecks.org/the-concerned-parents-toolbox>

[Building a Digital Defense for School Kids and Cell Phone Safety](https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-building-a-digital-defense-for-school-kids-and-cell-phone-safety) <https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-tech-tuesday-building-a-digital-defense-for-school-kids-and-cell-phone-safety>