FBI Phoenix
Jill McCabe
(623) 466-1844

August 8, 2018

FBI Tech Tuesday: Building a Digital Defense for School Kids and Cell Phone Safety

PHOENIX, AZ—Summer break is over, and it's time to pack up the backpacks and lunch bags for another school year. Many students are headed back to class with cell phones in their pockets. More and more kids are getting phones by the time they enter middle school—and some are toting their phones through elementary school hallways.

Cell phones are a great way for parents to keep in touch with their children. But, parents and kids alike need to recognize the risks that come bundled with that device. From scams to cyber bullies—if your child is old enough to have and carry a phone, then it's also time to have a conversation with him or her about potential risks.

Here are 10 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 the parent.
2. Parents should know every password to every device and every password to every app on that device. Sure you want your kids to have some privacy as they grow up, but they are still kids. You pay the bill, and as long as that child is a child, he or she is your responsibility.
3. Check those accounts—as well as instant messaging programs and texts—for disturbing content on a regular basis. You and your kids should have a

non-negotiable understanding that this access is a requirement for continued phone use.

4. Parents should make sure their child is using appropriate screen names. “Babygirl2005” and “sweet16” may sound cute and innocent, but they can be a beacon to predators.
5. Check the privacy and security settings on the phone and the apps. Check regularly to make sure they are up-to-date.
6. Learn about how photos are geo-tagged. Even if you are discreet about what you post, your photos could be tagged in the meta-data with your child’s exact location. Do you want just anybody to know what school your child goes to or what field his team uses for soccer practice? You should be able to turn this feature off in settings.
7. Teach your kids to never respond to calls, texts, or emails from unknown numbers or people. Scam artists and predators will victimize anyone, regardless of age.
8. Talk early and often to your child about the dangers that they may find on the other end of the line. If your child is old enough to carry a phone to school, he is old enough to have a frank discussion with you. Be open and responsive. If your child does encounter a bully or other disturbing content, you want him to feel like he can come to you to for help.
9. Talk to your kids about what constitutes appropriate language and photos. One sexually explicit photo can change a life forever. It is crucial that they understand that just because something starts out as a private communication between two people does not mean that it can't be shared with thousands of people in mere seconds.
10. Teach your children to program the privacy settings on social media feeds to the highest level and to reject any “friend requests” from those they don't know and trust in a face-to-face relationship. Parents should also consider forbidding any new “friend requests” by their kids, without parent approval.

If you or your child has been victimized by an online crime, make a report to the FBI. You can file an online report at the FBI’s Internet Crime Complaint Center at www.ic3.gov or call your FBI local office.