PARENTS' GUIDE TO SMART PHONE SAFETY

SMART or SCARY?

Smartphones are essentially little computers, so you might be a little worried when handing one over to your child. Take some time to understand the risks and implement a few safeguards so that you can help your child use smartphones safely.

THE RISKS

- **CYBERBULLYING**

With the constant connectivity of smartphones, your child may be more susceptible to cyberbullying or have more opportunities to cyberbully others.

- **GEOLOCATION**

A GPS-enabled smartphone can reveal your child's location through online posts and uploaded photos.

- **INAPPROPRIATE CONTENT**

With smartphones, your child has mobile access to content you may consider inappropriate, such as pornography or violent videos.

- **SEXTING**

Your child may use the Internet and social apps to send, receive, or forward revealing photos.

- **VIRUSES & MALWARE**

Just like a computer, a smartphone is vulnerable to security attacks if your child accesses unsecured websites and apps.

5 WAYS TO BE SMARTER THAN THE SMARTPHONE

1. Be a parent and a resource.
Establish clear guidelines, including time limits and consequences for inappropriate behavior, but be open so your child will come to you with any problems.

2. Set up smart security.
Smartphones today include a variety of security mechanisms including fingerprint scans, facial recognition and password locks. Enable these to protect access to the phone as well as apps with sensitive data.

3. Update the operating system.
New versions often contain important security fixes.

4. Approve apps before they are downloaded.
Make sure you understand their capabilities and approve their content.

5. Understand location services.
GPS features are useful when using maps, but you'll want to disable location-tagging when your child posts anything online.

PROTECTING YOUR KIDS ONLINE

CONNECT

Set some ground rules.
Establish clear guidelines like what types of sites kids can visit, apps they can download, and when they can have access to electronics. Consider "blackout" periods that require disconnection.

Research before you buy.
It's important to learn about a device's capabilities before you buy. Will it allow unknown people to communicate with my child? Will this allow children to make unchecked purchases?

Go beyond safeguards.
Installing monitoring software doesn't guarantee your child will be safe online. Time, attention and active conversation are the best tools to protect them.

LEARN

Know the platforms.
Online enticement happens across all platforms, so be aware of the sites, games and apps your children frequent. Ask them to show you how they use them.

Be proactive.
Teach your kids to spot common tricks used by online offenders. The most common tactics used to entice a child online were:
- Engaging the child in sexual conversation/roleplay as a grooming method.
- Directly asking the child for sexually explicit images of themselves, or offering to mutually exchange images.
- Developing a rapport with the child through compliments and other supportive behaviors such as "liking" their online posts.
- Sending unprompted sexually explicit images of themselves.
- Pretending to be younger.
- Offering incentives for explicit content.

Spot the Red Flags.
A child who is experiencing online enticement may be:
- Spending increasing time online.
- Getting upset when he or she is not allowed on their device.
- Taking extra steps to conceal what they are doing online.
- Receiving gifts from people you don't know.

ENGAGE

Talk about it!
Your kids might not tell you everything, but ask anyway. Regular conversations about safety can go a long way in increasing trust and communication.

Get involved.
Challenge them to a duel. If you have kids who like to play online games, ask if you can play, too. When you respect their interests, they're more likely to respect your rules.

Don't pull the plug.
Taking away internet access because they may have made mistakes online doesn't solve the problem. Talk to them about protecting themselves and respecting others online.

To schedule an informational session email cos.cv@fbi.gov

Resources for Parents & Educators

FBI:
FBI.gov/how-can-we-help-you

Take It Down
https://takeitdown.ncmec.org/

Netsmartz:
Missingkids.org/netsmartz

Common Sense Media:
commonsensemedia.org

Bark:
bark.us

ConnectSafely:
connectsafely.org

REPORT

What do you do next?

- Call local law enforcement
- Contact your local FBI Field Office - 216-522-1400
- Call or submit tip to NCMEC at 1-800-THE LOST or cybertipline.org
- Submit tip to FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov