Internet Safety Tips for Parents

1. Keep all computers in a centralized area of the home
    - Having a computer in a centralized area allows parents the opportunity to monitor more closely the internet sites your children visit.
2. Have your children turn in their phones each night before they go to bed
    - Collect the phones and tablets and return them the next day. This will keep children from visiting internet sites and chatting with strangers in the middle of the night while parents are sleeping
3. Turn off the WiFi at night
    - In the event that a child sneaks the cell phone or tablet from the parents room during the middle of the night, parents can monitor cell data times to see if their children are using their phones during a prohibited time. With the WiFi disconnected, a child will have to use cellular data to surf the internet. Also, a tablet that works solely on WiFi will not operate with it shut off.
4. Talk to your children and let them know you are concerned for their safety
    - The internet, cell phones, and technology has become a baby sitter for parents. Many parents do not have safety conversations with their children. Let them know the dangers that lurk the internet and make sure they do not friend or speak to anyone online that they do not personally know. Many predators pretend to be children so that they can friend your child. Children don't view online friends as strangers the way strangers were viewed as the creepy guy at a park. They think these virtual people are really their friends.
5. Any internet site with a chat function can be a dangerous site
    - While we don't want to scare parents, we do want to make sure they are aware of predators friending and chatting with children on various gaming sites (Fortnite, Roblox, Madden, etc…). Any game that has a chat function gives predators an opportunity to prey on children. If it connects to the internet, there is a potential for danger. Only allow your children to play games online with people they know personally, not virtually.
6. Tell your children to never, ever, ever send pictures or videos to anyone over the internet
    - Many predators will pretend to be children and they often ask children for pictures. They are very crafty and children do not recognize the harm in sending a picture. Once the image is on the internet, it cannot be taken back. Remind them that whatever they send is permanent. Even when someone they know says they will not send it or share it, they often do. Encourage them to ask a parent before sharing any images with anyone online.
7. Beware of vault apps
    - Vault apps are secret apps that can be downloaded on a phone. They act to hide photos, videos, and chats so that parents cannot see them. An example of this is the vault calculator app. It works just like any other

calculator; however, allows the user to hide on the back end of the app whatever information they want to keep secret.

- To recognize vault apps, parents can look at the size of the file on the device to determine the amount of memory it is using. For example, a calculator operates at 1mb. If they see a calculator using a higher storage amount, this should alert them that something is wrong. If they view an app that shows to be using a large amount of storage but there shows to be nothing in the app, there is a problem.

8. If your child becomes a victim of an online predator, do not delete anything
   - Often a parent will panic when they discover their child is a victim. They worry that their child will get in trouble for having pornography on their device or they fear the child will go to jail for sharing images of themselves. Parents often delete the contents on the device to protect the child. By doing this, they have deleted valuable evidence law enforcement needs to prosecute the predator. Law enforcement will never prosecute a child who is a victim of online abuse.
   - The parent should place the phone in airplane mode and call the police. Airplane mode prevents anyone from deleting the device via a cloud.
   - If the phone is off, leave it off. A signal can be sent via the cloud to delete the contents of the phone. Once powered on, the device receives the signal from the cloud and the entire phone is deleted. Leave the phone off and call the police.
9. My 3rd grader is too young to know how to hide content on their device!
   - Children these days are very tech-savvy. If they are not, the adult they are communicating online with will be able to help them hide the data. Don't automatically assume your children can not operate a device because of their age. They might be getting help from someone they are chatting with.

Talk to your children. Educate them on the dangers that are present online. If they mess up, do not destroy the evidence. Contact the police and let us help prosecute the predators that prey on children.

12 Most Dangerous apps for Kids

Apps are both convenient and a curse. They make our life easier while at the same time creating dangers for our children. Here are 12 of the most dangerous apps for kids:

1. Discord
   - This is a free app designed specifically for gamers. They can chat via voice or text on this app.
   - This is the number one app currently being used by online predators in the Houston area
2. Whisper

   - It allows you to post secrets anonymously and chat with other users in your area

3. Kik
   - This free app allows you to send texts/pictures without those images and texts being logged into the phone history
   - It allows people to get connected in your area with a common interest.
   - This app is used primarily to meet people for dating/hooking up.
4. Snapchat
   - You can capture images or videos and make them available for a specified time. After that, the image/video disappears
   - It is dangerous because kids feel they can send a sexually explicit image or text and it will disappear; however, nothing sent over the internet disappears. Someone is always capturing the image on the receiving end.
5. Vine
   - Allows users to watch and post 6 second videos
   - While most of the videos are harmless, occasionally, porn videos pop up into the feed, exposing children to harmful material
6. ChatRoulette and Omegle
   - This allows video chat with complete strangers. Nothing else needs to be said.
7. Tinder
   - Users post pictures and images they find attractive can be flagged. If someone flags you as attractive, the app connects the two.
   - These are primarily for hooking up.
8. Poof
   - Hides other apps on your phone. You can select which ones to hide and their icons no longer appear on the phone.
   - If you see the Poof app on the phone, ask them what they are hiding.
9. Vault
   - We discussed these earlier. They are used to hide messages, images, videos, etc..
10. Sarahah
    - Known to be a perfect tool for cyberbullying, this app allows you to send and receive messages without logging in. There is no age restriction for this app.
11. Yubo
    - Tinder for Teens
    - Allows teens to swipe who they like based on photos
    - This provides predators with everything they need to contact a child
    - There is no age verification, so children do not know who they are chatting with.
12. Skout
    - Skout uses locations to put people in contact with those nearby.
    - Allows them to chat, send photos, and virtual gifts.

While these are a few apps, new ones are created everyday. Just be mindful of the apps your children use and monitor their devices regularly for suspicious activity.

Tracking Devices and Apps

There are a number of good tracking devices/apps on the market that will allow parents to monitor the internet habits of their children. The apps can be tailored to whatever the need is of the parent. They can track children whereabouts, show internet sites visited, monitor time spent online, etc.. Some of these are paid subscription apps while there are many that are free. What I would recommend is that a parent Google "tracking apps" and read the reviews on each one to find the best fit for them.

How to Report

Parents should report any incidents of abuse/solicitation to their local law enforcement officials. In addition, they may report any tips to the CyberTipline at **Cybertipline.org** or **1-800-THE-LOST**