What dangers do your children face when they go online?

All who participate in activities online face risks when they use the Internet, including adults. The world is constantly changing with new technology available daily. It may feel overwhelming when we focus on the big picture, so let's break it down. We will focus on several dangers that you and/or your child may face when you go online: privacy, Internet predators, sexting and cyberbullying.

Privacy

Privacy is a concern that all parents have for their children. As responsible Internet users we can take steps to protect our digital content. In this portion of the resource we will discuss behaviors that can threaten our privacy, and behaviors that can strengthen our privacy.

Apps

Some of the apps you have downloaded can access your contact list, or camera, for example Facebook and Instagram. Most Internet users don't read the privacy terms for the app that they are downloading, unwittingly giving companies access to private information. Many of these apps sell the information to a third party, which can be used for advertising or marketing, or to spy on your Internet use. Just recently a popular flashlight app was discovered to be accessing user contacts, SMS messages, and other personal data. Why does a flashlight app need access to personal information? The answer is they don't. They want to collect data to make money, so they offer the flashlight app for free.

To protect yourself from pesky data gatherers, methodically check the Privacy Policy and Terms of Use for every app that you download.

For more information on data gathering check out this link:

http://www.huffingtonpost.co.uk/2015/02/20/weird-online-security-_n_6718880.html

Sharing Personal Information

How often have you clicked on a link for a free prize or a discount at a popular store? Every person has been duped at least once into clicking a link and giving away personal information. Then you later regret filling out that "free" survey, as your inbox fills up with spam. It is important to talk to our kids about what information is okay to share online and what information we should keep private.

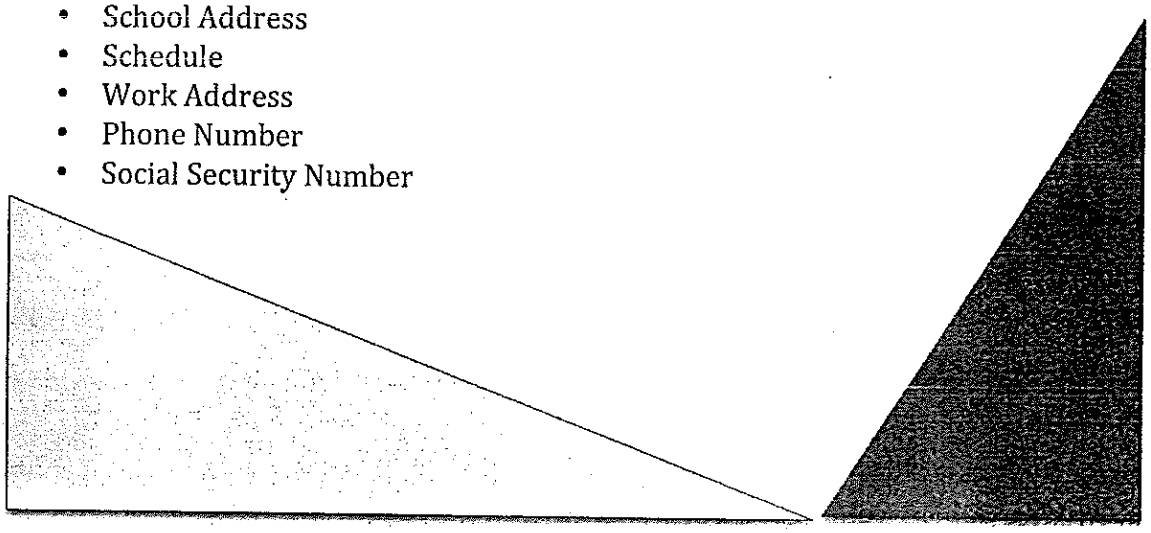
Responsible Internet users should do all in their power to keep their personal information private. As adults we often use secure sites to purchase items online, or fill out forms for insurance coverage, but our kids cannot always distinguish between safe and dangerous sites.

Younger children should be encouraged to always ask a trusted adult before sharing personal information on the Internet. You may have to teach your children specifically that they should not share their name, address, phone number, or school when online, especially not with a friend on a gaming website, social media, or other such instances.

Older children should be encouraged to verify the site is a safe place to share some personal information. (You probably will have to deal with your child getting a Facebook account.) Teens should be able to recognize that sites like Amazon, and university applications are okay, but that online gaming websites and other social media platforms will need to be vetted before divulging personal information.

Responsible Internet users should be cautious about sharing the following information:

- Name
- Address
- Financial Information
- School Address
- Schedule
- Work Address
- Phone Number
- Social Security Number



Sharing Inappropriate Information

We all had to go through the teenage phase; we all made stupid choices and learned from them. The difference between our stupid choices and teens' stupid choices is that ours were not public, and many teens today have their dumb choices broadcast for the world to see.

Parents should sit down with their kids and discuss inappropriate behaviors online. Teens need to know that it is not okay to post embarrassing photos or stories about their friends online, which could be considered cyberbullying. Also, teens can get into a lot of trouble for posting inappropriate or illegal pictures.

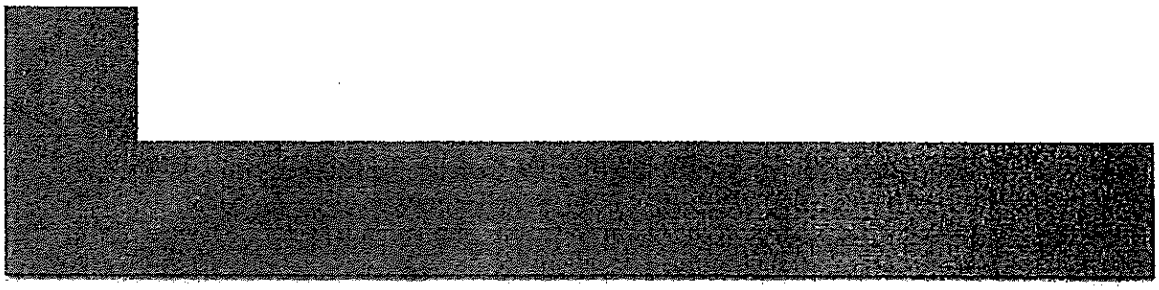
Many colleges are looking at teens' online behavior before they accept new applicants into their schools. Not only are colleges looking at online behavior, but also employers often check a candidate's online profile before hiring or interviewing a potential employee. That stupid choice that your teen made to go to a party where there was underage drinking could cost them their future.

Photo GPS Tagging

Not only are apps tracking and collecting data, sometimes our own phone cameras turn against us. Many smart phones have the capability to embed a GPS tag into every photo you take on your smart phone. That means, every photo you upload now lets every person who accesses the photo know the exact location you were in when you took the photo. So if you are taking an early morning selfie while getting ready, everyone now knows exactly where you live. Turning the GPS tag off is actually pretty simple.

For iPhone Users:

1. Click on the settings button
2. Click on the privacy button
3. Click on the location services button
4. Click on the camera button
5. Select the option "never"



For Android Users:

There are so many different android devices that there is not just one simple checklist. You will need to use a search engine to find the exact list for your specific phone.

Now your camera won't be sharing your location to all who can see your photo. Remember to check your tablet for the GPS tag as tablets and iPads can also tag your location when a photo is taken.

Gaming

Many children and teens are participating in online gaming. There are many different kinds of gaming options. Some games have chat boxes. It is important to sit down with your child and discuss online gaming safety. Some games only allow specific responses, and others allow free chat. Games with a free chat function could put your child in a dangerous situation. Internet predators can use these chat spaces to win a child's trust, and get private and personal information from them. Also, online gaming spaces can foster cyberbullies, who may harm your child emotionally. Encourage your child to share with you the games that they are playing, and the people that they are talking with to help them navigate the online gaming world.

Internet Predators

Many people imagine Internet predators to be an old creepy looking guy, who surfs the Internet in his basement, but in reality Internet predators are usually much younger. The average age for an Internet predator is 26 years old, which means that there are some that are older, but some that are quite a bit younger.

Internet predators are attracted to certain behaviors online. When students post inappropriate comments or pictures, particularly sexual in nature, they could draw the attention of an Internet predator. Some children are more at risk for running into a predator than others.

Netsmartz.org provides the following list of the type of children who are more at risk than others.

- Ages 13-15
- Mostly girls, but 25% are boys
- History of sexual or physical abuse
- Engage in patterns of risky behavior

Just because your child does not fall into this category does not mean that they will not run into an Internet predator. It is important to keep the lines of communication open between you and your child, so that they feel comfortable discussing with you the people they talk to online.

Children don't realize that they may accidently give away personal information when they are chatting with someone they think is their friend online. Say that your child was playing an Xbox or PlayStation game with someone that they don't know in real life. As they are playing, their younger sibling comes down and starts bugging them, trying to get their attention. In this instance your child is wearing a microphone while playing and chatting with the other player. Your child gets really frustrated with their sibling and shouts their name in frustration. They don't even realize that they just gave away their siblings name to a complete stranger.

In this situation the other player could just be another player like your child, but they could also be an Internet predator. It is important for your children to understand that not everyone is who they say they are online. People can pretend to be whatever they want to be online. Internet predators use gaming websites, but they also use other social media websites to meet kids online, such as Facebook, Instagram, Kik, Reddit, and any other social media app.

Grooming

Internet predators do all they can to win the trust of the child they are speaking to online. They call this behavior grooming. It is important to know the signs of grooming, so that you can teach your child how to recognize an Internet predator.

Netsmartz.org provides the following list to help a child recognize an Internet predator:

A predator who is trying to groom you might:

- Flatter you.
- Send you gifts, like cellphones or bus tickets.
- Discuss adult subjects, like sex.
- Ask you to keep secrets, such as not telling anyone about the relationship.
- Turn you against your family and friends. Predators want you to depend on them.
- Share or ask for revealing images.
- Blackmail you.

Keep an open line of communication with your children, so that they feel comfortable in discussing with you what they do online, and who they interact with online.

Reporting

If your child has shared with you that they are speaking to an Internet predator, or you suspect that they are speaking to an Internet predator, seek help immediately from your local police department.

If your child has a friend from another state that is speaking to an Internet predator, you can report the predator to Cybertipline.com.