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.

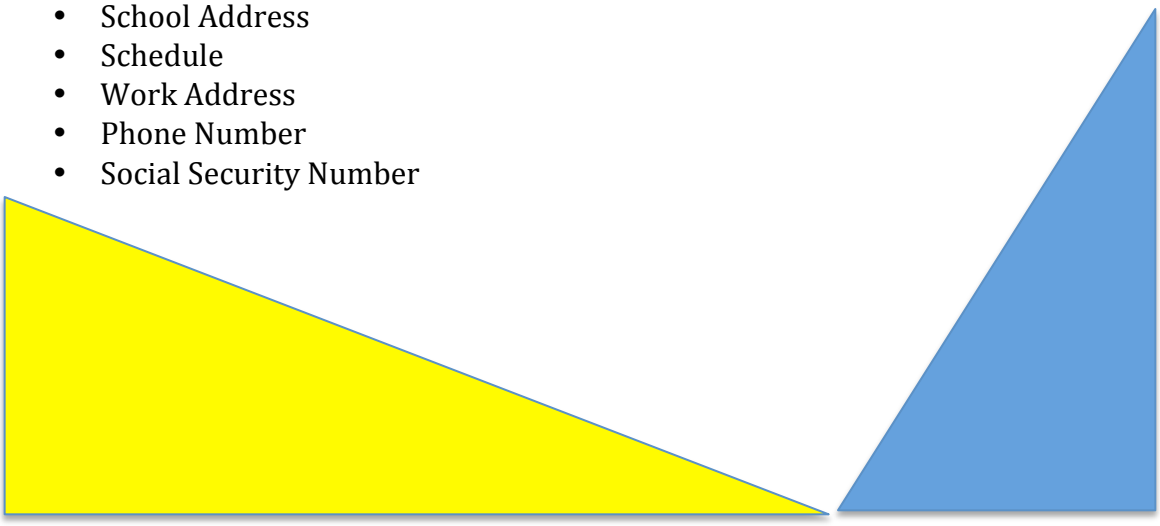
Responsible Internet users should do all in their power to keep their personal information private. As adults we often use secure sites to purchase items online, or fill out forms for insurance coverage, but our kids cannot always distinguish between safe and dangerous sites.

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.

Sexting

Did you know that the brain doesn't fully develop until age 26? As we got older, we can see more clearly the good and the bad choices we made when we were younger. Some teens are participating in a risky behavior called sexting. Sexting is sending sexually explicit photos or videos to others using the Internet.

Teens participate in sexting to be funny, impress a crush, and as part of their relationship with a boyfriend or girlfriend.

Whatever the reason that teens are sexting, it is still a dangerous behavior. Many teens are not aware that there are serious social and legal consequences for participating in this behavior.

Many teens don't think about the consequences before taking or sending the photo to a crush or friend. The consequences include, humiliation, blackmail, bullying/cyberbullying, suspension from school, or even police involvement.

Even though teens may not be charged with a serious crime, it is still a possibility. When teens send a sext they are creating child pornography. In the state of Utah, teens that are charged for offenses involving sexting have been charged with a misdemeanor and/or felony charges, depending on the individual situation.

It is important for you to keep an open dialogue with your teen regarding this issue. They may receive a sext from someone else, and they should feel comfortable talking to you about receiving this image.

If your child has received a sext, it is important that you document when the teen received the image, and that you document what your teen did with the image. Remind your teen that they should never forward an image to another person. Then you should report the behavior to someone in authority, police or school administration.

Images can spread very quickly on the Internet. Several teachers have done experiments to test the speed at which an image can spread via social media websites. One teacher had over 1.5 million views in 15 days. Discuss with your child the how quickly a sext could spread over the Internet.

Some teens sext because a significant other requests the image, but teens need to understand that that person is not thinking of their best interests. Discuss what a healthy sexual relationship looks like, and how to avoid damaging situations.

Cyberbullying

Have you ever wondered why people say extremely rude things online, but are really nice to your face? People will often say things online that they would never say in a face-to-face conversation because they can hide behind the computer.

What is cyberbullying? Stopbullying.gov gives us the following definition:

"Cyberbullying is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites."

Cyberbullying happens more often than we realize. Kids and teens can easily forget that saying something online is just like saying it face-to-face. It doesn't help that many reality TV shows and celebrities make bullying and cyberbullying seem like normal behavior. Kids need to understand that this behavior is not acceptable. Cyberbullying does not just manifest in one way, there are many different forms of cyberbullying.

Examples of cyberbullying provided by Netsmartz.org:

- Creating a hate group about someone.
- Posting mean comments online.
- Photoshopping someone's photo to embarrass them.
- Recording and posting fight videos.
- Spreading rumors and gossip through text messages.
- Stealing someone's identity to create a fake profile.

The Internet is vast and provides lots of opportunities for kids to bully others. As parents we need to be aware of sites and apps that foster cyberbullying. Staying informed is the best way that we can help protect our children.

The following chart lists popular websites and apps that can be places that foster cyberbullying.

Social Network	Website or App?	Age Limit	Features	Trouble Spots
Ask.fm Ask.fm	Free App; Online	13	Questions can be asked anonymously; can post videos	Cyberbullying on site is common; site doesn't monitor content
Badoo Badoo.com	Free App	18	Connecting with strangers; dating	Adult content
HotorNot HotorNot.com	Free App	13	Look at pictures of people; can rate others; chat with others	Chatting with strangers; adult content
Instagram Instagram.com	Free App; Online	13	Share photos and 15-second videos; share comments; can report inappropriate posts	Inappropriate photos; easy to network with strangers; if profile isn't private, anyone can access photos
Kik Messenger Kik.com	Free App	13 - 18 with "adult permission"	Free text messaging and photos, users can see if their text message was read; can block and report inappropriate posts	Strangers can message kids; messages can be sent out to strangers

Omegle Omegle.com	Free App; Online	13 - 17 with "adult permission"	Can chat with strangers who have similar interests	Chatting with strangers; can video chat; adult content
Pinterest Pinterest.com	Free App; Online	13	Tag or pin ideas of interest; look at others' content; craft ideas	Can comment on others' ideas within the site
Snapchat Snapchat.com	Free App	13	Share photos which only exist for up to 10 seconds, then are deleted by the site	Screen shots will save an image which can then be passed along
Tumblr Tumblr.com	Free App; Online	13	Users can blog text, photos, links, audio, video, and can chat with other users	Inappropriate content
Twitter Twitter.com	Free App	13	Post brief messages in real time; can follow tweets of others, especially celebrities	Tweets are permanently in cyber space; able to post location
Vine No online site	Free App	17	Post 6 second videos; share them	Easy to find adult content; all videos of people you follow are visible on your page
Whats App Whatsapp.com	App for Smartphones Only	16	Cross platform mobile messaging without the need to pay for texting; can only text your existing contacts	Cyberbullying on site is common; site doesn't monitor content

Words with Friends zynga.com/games/words-friends	Free App; Online	13	A Scrabble-type game where users play against others	The game can match players with opponents who are strangers; either player can initiate a chat, and there is no way to turn it off or filter the language
Yik Yak Yikyakapp.com	Free App	17	Online "bulletin board"; posts are limited to those in a 1.5 mile radius of the user	Cyberbullying and harassment are common; anonymous posts can be read by all

http://www.penfield.edu/BayTrail.cfm?subpage=1833780

How to tell if your child is being cyberbullied or is the cyberbully

It is important to know the signs of whether your child is being cyberbullied or whether they are the actually the cyberbully. Bullying happens all the time and we need to be aware of our child's behaviors. Parents should take action if they sense that their child is being bullied or is bullying someone else.

How can we determine if our child is being bullied or being the bully?

Netsmartz.org provides the following signs:

- **How to tell if your child is being cyberbullied**

- Suddenly stop using the computer or cell phone.
- Act nervous when receiving an email, IM or text.
- Seem uneasy about going to school.
- Withdraw from friends and family.

- **How to tell if your child is being the cyberbully:**

- "Quickly switch screens or close programs when you walk by.

- Use the computer at all hours of the night.
- Get unusually upset if they cannot use the computer.
- Laugh excessively while online.
- Avoid discussions about what they are doing.
- Use multiple online accounts or use an account that is not their own."

Another group of kids involved in cyber bullying is the bystander group. This group sees the bullying incident happen. The interesting thing is that the bystander group has the most power to help stop bullying and cyberbullying incidents. We need to teach our kids about the power of standing up against bullies. When we choose to ignore bullying we are choosing the side of the bully.

Teaching your children the power of standing up for others is important for us as a society. Bullying doesn't stop just because a person becomes an adult. If we teach our kids the importance of standing up against bullies when they are young, they will continue to stand up for others when they get older.

What to do if your child is cyberbullied

If your child is being bullied there are steps that need to be taken. We need to report the incidents to administration and sometimes we may need to go to the police. We need to save evidence from online bullying incidents, so that when we report it we can show proof to administration or the police.

The following tips will help parents, and students in bullying situations:

- Block or ban the bully
- Don't respond to the bully
- Save the evidence
- Shut down an old account or create a new account
- Tell a trusted adult
- Report

How to communicate with your child about Internet safety

Talking to your child about Internet safety issues may seem like a daunting task, especially since many parents feel that they don't know about the latest apps or websites their kids find interesting. As parents we can parent our kids on the Internet.

Beth Blecherman gives the following fantastic advice on how to start the conversation with your child.

> "1. Educate yourself first, then talk to your kids about Internet safety.
>
> 2. Start conversations early, but remember it's never too late to start.
>
> 3. Make a plan to have regular "talks."
>
> 4. Use of tech should include creating and engaging in content.
>
> 5. Establish family rules."
>
> http://dotcomplicated.co/content/2013/06/internet_safety/

As we keep an open line of communication with our children, we can be a resource to help them as they go forward with their digital future.

For information on how to talk to your kids about pornography use the following link:

http://www.nytimes.com/interactive/2012/05/10/garden/porn-intro.html?ref=garden&_r=1&

It is important for our kids to feel comfortable in talking with us about anything. Our kids will make mistakes, or run into inappropriate material on the Internet, and the most important thing is that they can talk with us about the mistakes that they make and content that they run into when online. Inappropriate content is readily accessible to anyone with an Internet capable device.

Some parents take away the Internet or phone use when their kids inappropriately use the Internet. This actually creates more problems than it solves. If your child feels that you will take away the phone when they talk to you about

problems they face online or mistakes they have made, they will choose not to talk to you about it. If your child has made a very bad mistake, find another way to discipline your child, taking away the phone will only distance them from you.

If your child comes to you after they make a mistake online, how you respond is very important. Here are some ideas on how to respond to your child:

1. Don't take away privileges for online use
2. Listen attentively
3. Don't get angry
4. If a punishment is necessary take away another privilege
5. Talk about ways to ensure this doesn't happen again

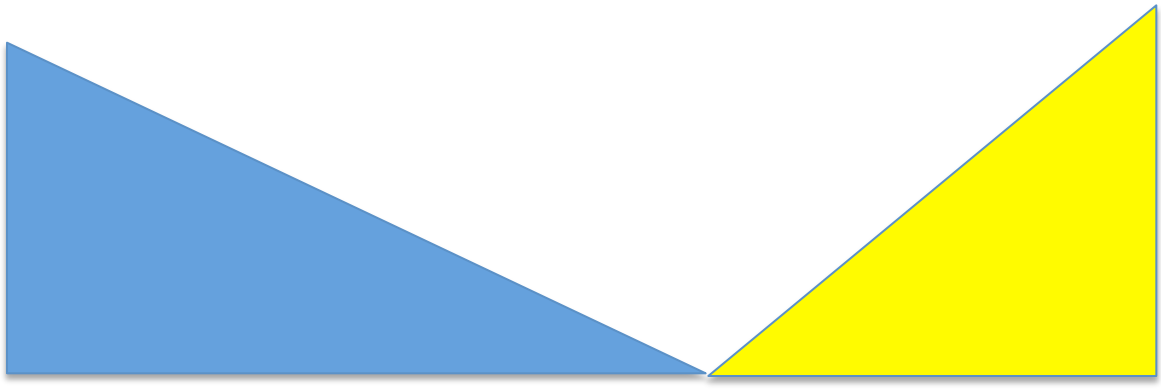
As parents we can help guide our kids to a positive digital future. We should not stop parenting because your child is online. As parents we can take action to protect our children against dangers found on the Internet. Janelle Burley Hofmann created a contract with her 13 year old when he got his first iPhone. Her contract is comprehensive and very helpful. Parents can modify the rules so that they fit their own households.

The following is a copy of Janelle Burley Hofmann's contract.

"Dear Gregory

Merry Christmas! You are now the proud owner of an iPhone. You are a good & responsible 13 year old boy and you deserve this gift. But with the acceptance of this present comes rules and regulations. Please read through the following contract. I hope that you understand it is my job to raise you into a well rounded, healthy young man that can function in the world and coexist with technology, not be ruled by it. Failure to comply with the following list will result in termination of your iPhone ownership.

I love you madly & look forward to sharing several million text messages with you in the days to come.



1. It is my phone. I bought it. I pay for it. I am loaning it to you. Aren't I the greatest?

2. I will always know the password.

3. If it rings, answer it. It is a phone. Say hello, use your manners. Do not ever ignore a phone call if the screen reads "Mom" or "Dad". Not ever."

Click the link below for the full contract:

http://www.janellburleyhofmann.com/the-contract/

Monitoring Software

Every household will deal with Internet safety differently. Some parents may also desire to add monitoring software to their children's devices. Here is a list of potential software to assist in monitoring your child's Internet activities.

- "**ChildwebGuardian** screens page content for keywords and phrases, blocks blacklisted sites, allows for Internet use restrictions according to days and times, stores URLs of visited pages, sends reports via e-mail, restricts access to approved sites only, and allows gaming restrictions by day and time.
- **CyberPatrol** provides parents with parental controls allowing for web filtering, online time limits, Internet activity monitors, chat and IM restrictions, and program blocking.
- **CYBERsitter** includes remote monitoring, Facebook and Twitter activity recording, user-specific content filter controls, user-specific time schedules, different content filters for different members of the family/age groups, and the capability to block specific applications from accessing the Internet.
- **eBLASTER** records e-mails, social media messages, chat and IM, keystrokes, web browsing activity, applications run, and log on activity.
- **McAfee safeeyes** filters web, video, and music content; and also creates reports that include Internet search activity, IM activity, and social network use.
- **Net Nanny** provides parents with the capability to filter Internet content, block adult content, set usage time limits, monitor social media activity, monitor IM and chat room use, mask inappropriate language, and receive cyberbullying alerts.
- **Norton Family** provides families with smartphone monitoring; web monitoring and blocking; and capability to set time limits, monitor social network activity, track Internet searches, and receive e-mail alerts.

- **Avira Social Network Protection** scans activity and alerts parents to contact from strangers, potential cyberbullying, inappropriate content, and reputation risk.
- **Windows Live Family Safety** provides family safety filters, website preference settings, and Windows parental controls.
- **iboss Home Parental Control Router** offers a wireless router with filter functionality that acts as a firewall for all devices connected to the Internet through that router.
- **Identity Guard** offers a variety of identity-monitoring services along with Internet monitoring, public record monitoring, credit monitoring, and more. Identity Guard also offers kID Sure, a product designed for child identity–theft monitoring.
- **LifeLock** provides identity theft monitoring, credit- and noncredit-related alerts, monitoring for exposure of personal information, and comprehensive identity theft recovery services."

http://www.dummies.com/how-to/content/parental-tools-to-monitor-and-protect-your-digital.html

The Internet is full of dangers, but it also holds a wealth of information. We should never let fear stop us from using this great resource, but we can take steps to help protect and enable our children to navigate the web safely.

Additional Web Resources

1. Netsmartz.org
2. Commonsensemedia.org
3. Stopbullying.gov
4. Parentesource.com
5. Eyesonbullying.org
6. Kidpower.org