Internet Safety
By: Lucinda Thelen M.Ed., CAPE

Children use the Internet to:

- do their homework,
- play games
- socialize with their peers.

Benefits:

- support learning and social interaction.
- accessible design and simplified language,
- instantly available video clips.
- opportunities for learning through repetition
- easier than face to face communication.
    - use of consistent and easily recognizable emoticons replaces the need to decode people's body language, facial expressions and vocal tone that can be problematic in personal communications.
    - Allows more time to respond

While there are many benefits to using the internet, there are also risks and with easy access to the internet, they must learn about these risks and how to protect themselves.

Risks:

- Cyberbullying
    - Cyberbullying is the use of technology to tease, humiliate, threaten and/or harass someone
- Geolocation
    - Figuring out who and where you are
- Inappropriate content
    - Violence, pornography, illegal behavior and hate speech
- False Information
    - The Internet allows anyone anywhere to publish anything everywhere.
- Sexting and grooming
    - Sexting is the sending or distributing of nude or partially nude images
    - Setting someone up to be a sexual target
- Viruses and malware
    - Programs that damage or steal data
- Identity Theft
    - Enough personal information is acquired to have another individual pretend to be you (financial and reputation)
- Digital footprint
    - Information you leave on the internet (photos, messages, videos, texts) Can haunt you forever
- Health
    - Sedentary (weight, carpel tunnel, posture), vision, addiction, sleep problems,

All children are vulnerable online but for some of our children they may have difficulty recognizing threats and threatening behavior. As a parent you are the first line of defense so here are some **general guidelines**

Make your home network safe

- Keep it public- keep computers/tablets/phones in a shared place where you can monitor online behavior
- Filter content- Install filters (google safe search) and set up parental controls
    - http://www.toptenreviews.com/software/security/best-internet-filter-software/
    - **https://www.howtogeek.com/167545/4-ways-to-set-up-parental-controls-on-your-home-network/**
- Increase security- used updated virus protection and firewalls
- Use child friendly browsers
    - **https://www.commonsensemedia.org/lists/kid-safe-browsers-and-search-sites#**

Teach online behavior

- Establish ground rules- Identify what is okay to do online and what is not
    - TEAM approach- Talk, Explore, Agree, Manage
    - Contract or rule list
    - Follow up
- Information sharing- What is safe and what is not
    - Do not share list
    - Set up password protection
- Netiquette-
    - No rudeness or meanness (all caps, name calling, forwarding information)
- Legal Issues
    - Your child can also be cyberbully and post inappropriate messages and pictures
    - Teach them what is illegal, especially when they are over 18, and what consequences can occur.
- Resources & Support
    - **http://www.netsmartz.org/SpecialNeeds (in Spanish too)**
    - Give them a lifeline- keep communication open
    - Roleplay and practice responses to possible threats
    - Google- Be internet awesome https://beinternetawesome.withgoogle.com/
    - Brainpop Digital Citizenship https://www.brainpop.com/digitalcitizenship/
    - **Connect Safely** - http://www.connectsafely.org/ Provides online advice for parents about technology and how to use it safely. Particularly useful is the downloadable parent's guide to Facebook and Snapchat.
- False Information
    - Just because it is on the internet that doesn't mean it is true
    - Watch for "sponsored content"
    - Look at URL- .co instead of .com or misspellings
    - Check the source (about us section)
    - Double and triple check the facts!

- fact- and bias-checking sites
    - Snopes. This independent, nonpartisan website run by professional researcher and writer David Mikkelson researches urban legends and other rumors. It is often the first to set the facts straight on wild fake news claims.
    - https://smhoaxslayer.com/ - another credible website that's known to debunk false stories, fake news, viral internet rumors and urban legends. There's actually also a dedicated section on the site that lists many weird and hard-to-believe emails and viral stories that are actually true for a change.
    - Politifact. This Pulitzer Prize winning website rates the accuracy of claims by elected officials. Run by editors and reporters from the independent newspaper Tampa Bay Times, Politicfact features the Truth-O-Meter that rates statements as "True," "Mostly True," "Half True," "False," and "Pants on Fire."

Now let's review the risks again in more detail:

Cyberbullying (Cyberbullying is the use of technology to tease, humiliate, threaten and/or harass someone)

- It can take place through text messaging or social media. Cyberbullies might send mean comments, post embarrassing photos, or share private information about someone to humiliate or mock them online. Even if your child isn't being cyberbullied, remind them that it is everyone's job to prevent bullying and encourage them to take a stand
- Signs of being cyberbullied
    - Avoids using internet
    - Seems stressed or anxious when getting emails or messages
    - Withdraws from family and friends
    - Resists attending family or school functions
    - Shows signs of depression, low self-esteem or fear
    - Declining grades
    - Trouble eating or sleeping
    - Serious case- considering suicide
- Teach your child these responses
    - Don't respond to messages
    - Save the evidence
    - Report it
- If they see someone else being cyberbullied
    - Do not forward embarrassing messages or photographs
    - Do not comment on insulting or harassing posts
    - Report it
    - Support the victim by being a good friend

Teach Privacy (this addresses Identity theft, geolocation, and grooming)

- Going on the internet is like going out on Halloween
    - Everyone's face is hidden
    - Unless you know your friends costume (online name) you don't know if you're talking to your friend (john doe is not John Doe)
    - Any stranger can pretend to be a friend and knock on your door
- Do not share
    - Email
    - Full name
    - Location or phone number
    - School name
    - Passwords or any personal information
- Ways you make share information unintentionally
    - Usernames
    - Geolocation
    - Pictures
- Tricks to get you to share
    - Pop-ups
    - Friend requests
        - Remember circle of friends
        - Only give information to inner circle
    - Fraudulent websites or links
        - Looks for https:// or lock in browser window
        - Use google safe search
        - Know your domain
            - .edu- school, college or university
            - .gov- government agency
            - .com- commercial business (make sure it's legitimate)
            - .net- network
            - .org- advocacy organization
- Parental Responses
    - Check comments and images for personal information and inappropriate content, teach them, then delete.
    - Look at contact lists. If you don't know them check what they are sharing to make sure it is appropriate
    - Check privacy settings

Inappropriate Content

- Set the rule- If you see something that makes you uncomfortable, sad, scared or confused
    - Hit the back button
    - Turn off the screen
    - Tell a parent or authority figure

- Parent actions
    - Check browser history
    - Talk about what they're doing
    - Keep it visible
- Trolls- stir trouble on purpose
    - Don't respond (Don't feed them)

Sexting and Grooming

- Messaging, chat rooms, social media are feeding grounds for perpetrators
    - The intent can be to embarrass, humiliate, bully or assault
    - If the person is not a close circle friend- give out no personal information, no matter how "friendly" they are.
    - No face to face meetings
- Watch for changes
    - Increasing online time
    - Getting upset when not allowed on device
    - Taking extra steps to conceal what they're doing online
    - Receiving gifts or pictures from unknown people
- Social Spaces (Facebook, chatrooms, text messages) are like a house
    - Do you open the door to strangers? No- so why friend them or even have your address public?
    - Who do you let into your house? Your social media page or apps are your living room- that is for friends and family
    - Bedroom-this is a private place- very few people should enter. This means sharing about your personal feelings, wants, needs and details.
    - Bathroom- This is off limits to anyone but you!! No one should ask for any information or pictures about your body.
- Parental responses
    - Actively listen, do not look shocked or disbelieving.
    - Stay calm.
    - Take what they are saying seriously.
    - Do not ask for detail.
    - Reassure them that they are doing the right thing.
    - Do not promise to keep secrets.
    - Tell them that you will have to share this information.
    - Explain what will happen next.
    - Be familiar with your child protection procedures.
    - Record the information as quickly as possible – facts not opinion.
    - Sign and date everything you record.
    - Get support for yourself.

Digital Footprint (the portrait of who you are online)

- What is shared is shared forever (photos, messages, videos, texts)
    - Your skype calls, comments on social media, app use, and emails can be seen by others or tracked in a data base
    - This information can be shared with others, looked at by potential employers, and used to harm you.

- Parental Responses
    - Teach that whatever they post or look at is not private and they should be okay with anyone seeing it.
    - Have them imagine that what they write or what pictures they share could be shared anywhere in the world.

Viruses or Malware

- Protect your computer with up to date virus protectors or firewalls
- Don't respond to pop-ups or open attachments
- Don't click on links you don't know are protected no matter who they come from
- Don't answer or open spam emails
- Update apps to get latest protection
- If contacted that there is an issue- contact the company directly

Health (physical issues, sleep disturbance, vision and addiction)

- Set time limits for where, when and time length of the device use
- Establish clear guidelines of use and be consistent
- Establish consequences

Additional Information

- **Apps**
    - Online safety information: https://www.nspcc.org.uk/keeping-children-safe/online-safety/
    - Adjust privacy settings
- **Smartphones/tablets**
    - Zombie phones become alive with Wi-Fi
    - Understand location system and disable for apps and posting on line
    - Learn acronyms
    - Control nighttime use

Are they ready for a cell phone?

- Can they keep up with its location?
- Remember to charge it?
- Can they avoid damaging it?
- Will they respect and understand the limits on the phone's plan?
- Will they check for and respond to messages?
- Will they follow rules for cell phone use at home, schools and public places?
- Will they understand what harassment and inappropriate contact look like?
- Can they understand and use emojis and abbreviations appropriately?
- Do you as the parent have enough time and interest to teach your child how to use their phone?

- **Gaming**
  - Know safety features
  - Keep consoles in an easy to supervise location
  - Set rules for how long they can play, what types of games they can play and who else may participate
  - Use the Internet Software Rating Board http://www.esrb.org/

Nothing matters more than protecting your child, both in the digital sphere and in the real world. Use these tips and best practices to create a safe, positive online experience for your child.