Navigating a Digital Maze:
An Online Safety Guide for Parents

Our children are the greatest gift and the greatest responsibility we have been given. We shepherd them with wisdom and care through their years as they mature from childhood through their teen years. Now more than ever, this navigation requires attentiveness on the part of parents.

Parents need to understand the digital age and the technology it offers for learning and expanding their student's world. It is equally important for parents to understand this world can bring new challenges and potential hazards if improperly used. This booklet attempts to provide parents with an overview of the digital world and what they need to know to help their child navigate the digital maze with safety and good judgement.

Nebraska Attorney General's Office

AGO.Nebraska.gov

402-471-2683

Sextortion:

- Sextortion occurs when a scammer convinces a victim to send explicit photos and then blackmails that victim with that content and demands money, sexual activity, or additional sexual content.

- The victim's fear that somebody might share their private images or information with their parents, family, and friends can be intense enough to create suicidal thoughts for a victim or other mental health related issues. Sextortion has resulted in a loss of life for victims of all ages.

- Talk to your kids about the risks of sending sexually explicit photos, videos, or other compromising information, even to people who seem trustworthy. Sending these items allows a predator to share them with someone else, even after the victim decides they do not consent anymore.

- If your child has been the victim of sextortion, please contact your local law enforcement or the Omaha FBI Office at (402) 493-8688. You can also visit NCMEC's webpage for more information about sextortion and removing your child's images from the internet.

Grooming & Online Enticement:

- Predators groom children online. These individuals have easier access to one-on-one conversations with your child over the internet.

- Setting up parental controls on your child's phone and monitoring their activity is the first step in prevention, but it is important to talk to your child about forming healthy relationships, especially with those they meet online.

- Keep in mind that most child abuse occurs with a person who the child trusts, such as a family member or friend, and not a stranger. It's important to set boundaries with family members and friends in addition to new acquaintances.

- Let your child know they should talk to you about anyone seeking repeated one-on-one conversations with them, asking them to keep secrets, or pressuring them into sexual conversations.

- If you have reason to believe someone is enticing your child online, report it to law enforcement immediately.

Setting Passwords:

- Not all passwords are created equal. Create passwords that are long and strong using at least 12 characters and a combination of numbers, letters, and symbols.

- If you use a special character besides an exclamation point, the password becomes dramatically harder to crack.

- Talk to your child about what passwords they are and aren't allowed to have and the importance of keeping them private.

- There are password strength checking websites that can help you determine if your password is strong enough.

Social Media Apps & Parental Controls:

- Research any app your child downloads, even if it appears innocent. Many apps come with parental controls or privacy settings that can be used to create healthy boundaries for your child. There are parental controls on your child's phone that can restrict your child from downloading new apps without your consent.

- Any minor using social media accounts or other apps should have their account set to "private" and their location services turned off. Research each platform to understand how to activate or deactivate these settings.

- There are several ongoing lawsuits against social media companies for harming children through addictive products and algorithms. There is evidence to indicate that social media companies do not prevent children from consuming content relating to eating disorders, suicidal thoughts, and other concerning topics.

- Consider the potential risks when deciding whether to allow your children to use social media.

Social Media Apps & Parental Controls:

- Legally, social media companies are limited from collecting data on children under 13 due to The Federal Trade Commission's Children's Online Privacy Protection Act (COPPA).

- Many kids have secret social media accounts in addition to the account a parent may be following. Kids may be sharing content on these accounts that they wouldn't share on accounts their parents and family follow.

- Some apps are risky regardless of the settings. Apps with disappearing photos and chats or apps that intentionally create situations for children and strangers to interact are dangerous.

Cyberbullying:

- Cyberbullying can severely impact a child's self-esteem. Ask your child if they can think of a safe person to talk to if they experience bullying online.

- Talk to your kids about the value of being an upstander—someone who defends someone who is being bullied online.

- Check with your child's school to learn more about their protocols and procedures for cyberbullying.

- If someone is harassing your child, encourage them to remove that person from their friends list, block their username or email address, and report them to the site administrator. If your child finds a profile that was created or altered without his or her permission, contact the site to have it taken down.

- If your child is experiencing suicidal thoughts due to cyberbullying, call or text the Suicide & Crisis Lifeline at 988 or contact law enforcement immediately.

- Visit Stopbullying.gov for more information on how to respond to and prevent bullying.

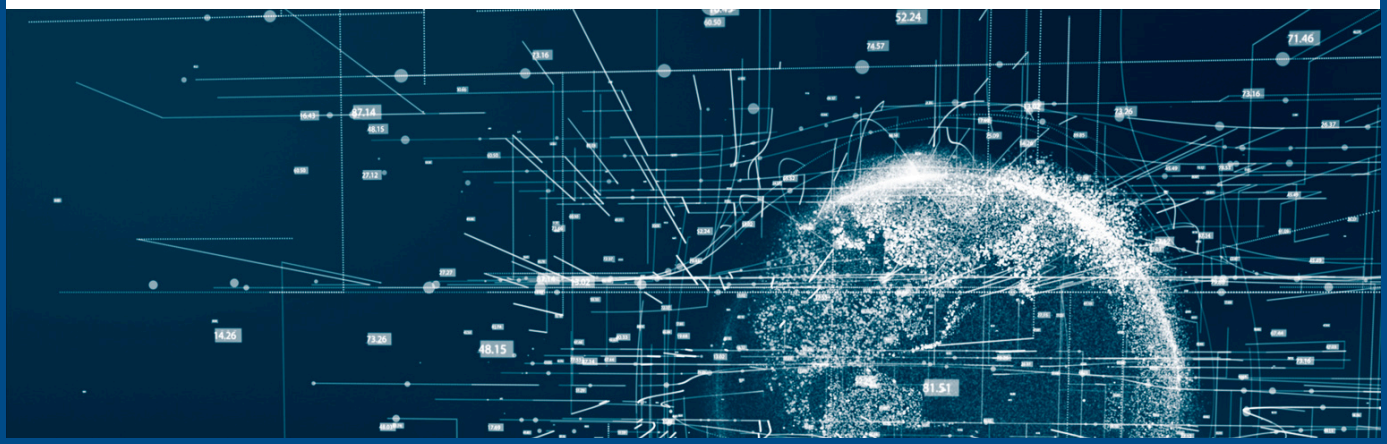
AI - Artificial Intelligence:

- AI is rapidly developing. There are many unknowns when it comes to AI from a child online safety standpoint.

- AI can mimic voices, alter photos, and create additional content. The content AI can create may not be content that you want of your child, including explicit content.

- Keep in mind that the more information available online about your child, the more potential content someone can manipulate.

- Consider limiting what you post of your children online to protect them. There are private photo sharing apps available if you wish to share updates of your child with family and friends without posting their image to social media.



Digital Footprint:

- Your digital footprint is the trail of data you leave when using the internet.
- It is essential that your child is set up for success. Help them understand the permanency of the internet and how content can be challenging to remove.
- Talk to your child about creating a positive digital footprint. Ask them what kind of person they want to be online and how they wish to be known.
- Be careful with what information you child shares online with websites, apps, and social media. If they must share personal information, do so only with trusted friends.
- Teach your children it is better to handle disagreements in person rather than online.
- The Nebraska Attorney General's Office has two videos designed to educate middle school and high school students on the importance of leaving a positive digital footprint.