# A COMPREHENSIVE ONLINE **SAFETY GUIDE** FOR PARENTS

THE
LANTERN
PROJECT

# TABLE OF CONTENTS

# INTRODUCTION

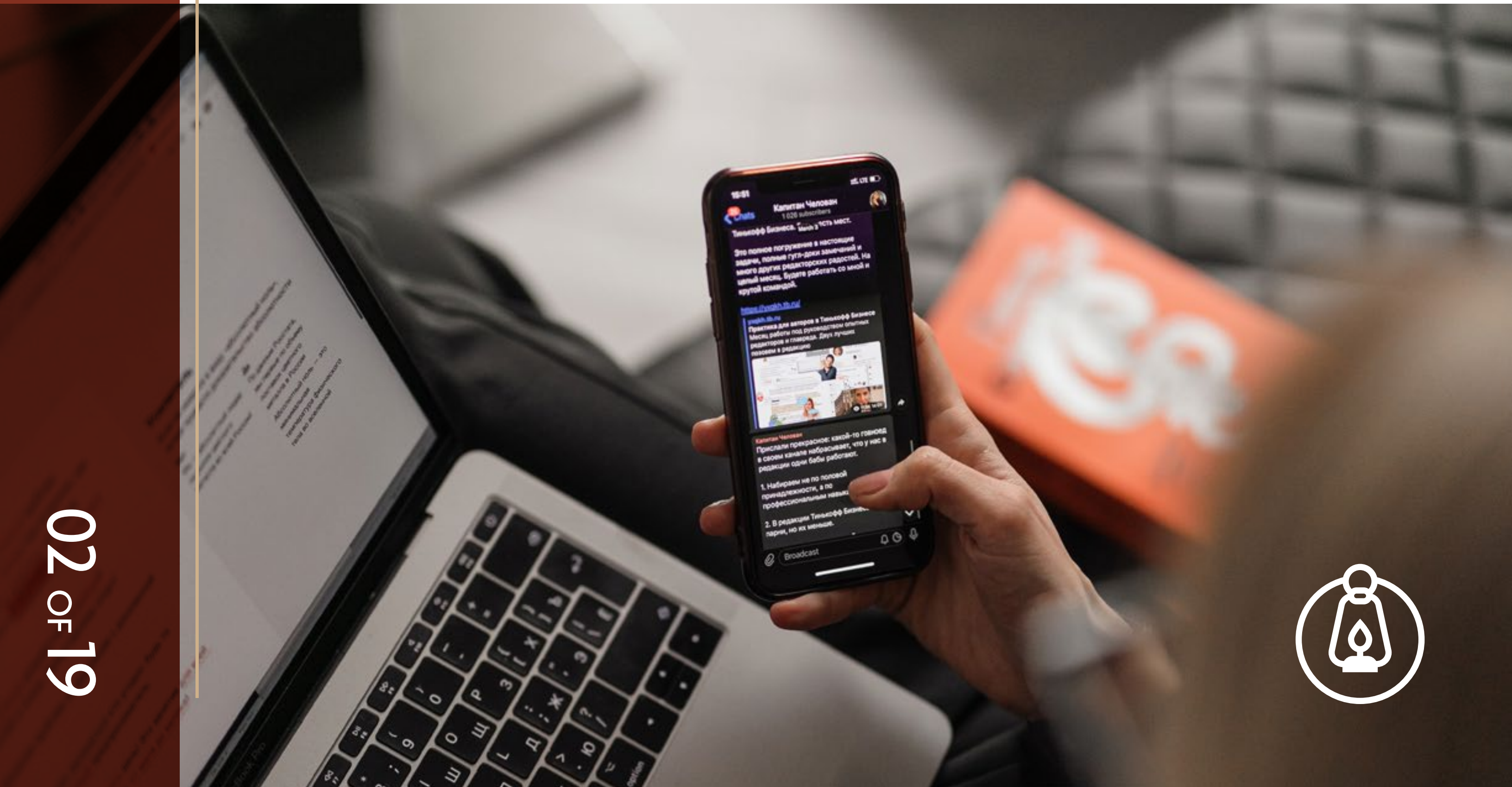
Today's world looks much different than the one we grew up in. Our children are bombarded with technology on a daily basis through virtual learning, communicating with friends, streaming media, and interacting on social apps. Because technology is ever changing and advancing at a rapid pace, many parents feel overwhelmed and unable to keep up with monitoring their children to keep them safe online. That's where The Lantern Project steps in-- we're here to aid parents in protecting their kids online by taking the guesswork and uncertainty out of the equation. We stay up to date on advances in technology so you don't have to.

We aim for you and your children to:

- Create open and safe dialogue regarding technology use
- Implement age-appropriate family guidelines and agreements regarding devices
- Be aware of online predators and suspicious behaviors
- Understand the consequences of inappropriate use
- Maintain a positive and responsible digital footprint

It's important to remember that children's age and maturity play a role in their use of the internet and media, so a one-size-fits-all approach will not work when it comes to safeguarding devices and monitoring usage. It's our goal to provide you with a framework of realistic expectations and boundaries that are age-appropriate for your children. As their parents and guardians, it is ultimately up to you to determine if this framework applies to your family.

> *…it is absolutely completely possible to make different choices about technology from the default settings of the world around us….it is possible to love and use all kinds of technology but still make radical choices to prevent technology from taking over our lives.*
>
> –Andy Crouch, author of The Tech-Wise Family



# MODELING BEHAVIOR

**We can’t stress enough the importance of parents setting an example for their children. If you are constantly distracted with your phone or tablet, you can’t expect your child to do otherwise. It is common for our children to mimic the behavior they see, so we strongly encourage you to evaluate your personal habits and modify as necessary.**

Consider these behaviors:

- Do you have boundaries or downtime/screen free times?
- Do your children constantly have to repeat themselves or beg for your attention while you’re on your phone?
- When posting online avoid oversharing personal information, bullying, or engaging in drama.
- Think before you post: if sharing a photo or video of your children, run it through the filter of “would it be appropriate for a stranger to see this?”· Avoid photos involving nudity or partial nudity, bathtub photos, or photos/videos in which the child is wearing age inappropriate or revealing clothing. While many photos/videos may be entirely innocent in nature, there are many predators out there who view them through a much different (and less innocent) lens.

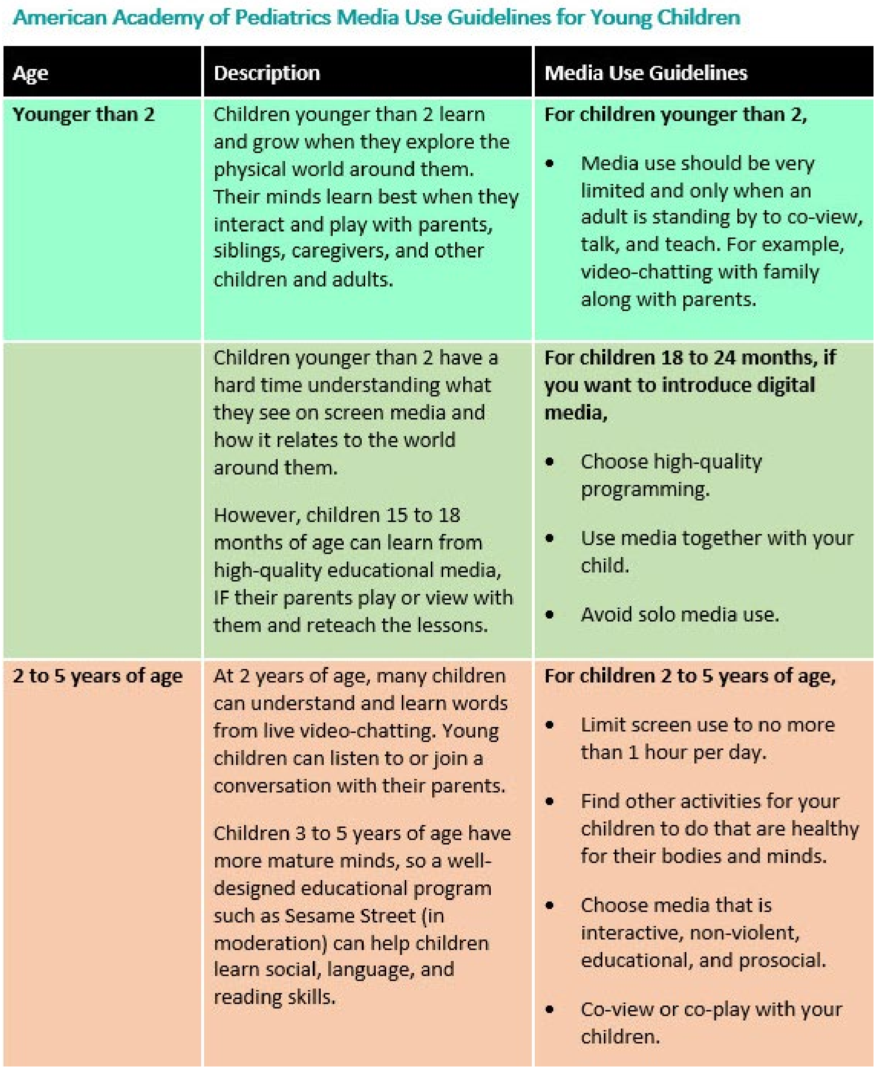
**Setting expectations and boundaries is an essential foundation for media safety. It's important to implement age appropriate guidelines, which means the rules can vary from child to child within your household. A Family Media Values Agreement is a great place to start, as this set of guidelines will determine what is considered acceptable vs unacceptable behavior for their devices. It is necessary to establish that devices are a privilege and in order to use them they must follow the rules you set and/or agree upon.**

Click here for an example of a customizable Family Media Guide.

Considerations:

- Time limits on devices
- Create tech free zones (ex. No devices in private spaces such as bedrooms and bathrooms or create a charging station in a central location to avoid overnight access)
- Require access to devices and knowledge of their passwords
- Explain the importance of keeping certain information private and help them set privacy settings on apps
- Ask them to show you the apps they use, the websites they visit, and the people they communicate with. Keep an open line of communication on these fronts.
- Discuss safe interactions and relationships
- Define appropriate vs. inappropriate content and behavior

- Define appropriate vs. inappropriate images
- Determine which apps are allowed vs. restricted
- Set specific boundaries that are non-negotiable (no bullying, no sexting, no inappropriate language, no pornography, etc.)
- Stress the importance of communication and remind your kids that you want them to come to you with any concerns or questions
- Commit to setting boundaries for yourself and modeling appropriate online behavior
- Decide if additional parental control software is necessary for monitoring



American Academy of Pediatrics Media Use Guidelines for Young Children

| Age | Description | Media Use Guidelines |
|---|---|---|
| Younger than 2 | Children younger than 2 learn and grow when they explore the physical world around them. Their minds learn best when they interact and play with parents, siblings, caregivers, and other children and adults. | For children younger than 2,<br>• Media use should be very limited and only when an adult is standing by to co-view, talk, and teach. For example, video-chatting with family along with parents. |
| | Children younger than 2 have a hard time understanding what they see on screen media and how it relates to the world around them.<br>However, children 15 to 18 months of age can learn from high-quality educational media, IF their parents play or view with them and reteach the lessons. | For children 18 to 24 months, if you want to introduce digital media,<br>• Choose high-quality programming.<br>• Use media together with your child.<br>• Avoid solo media use. |
| 2 to 5 years of age | At 2 years of age, many children can understand and learn words from live video-chatting. Young children can listen to or join a conversation with their parents.<br>Children 3 to 5 years of age have more mature minds, so a well-designed educational program such as Sesame Street (in moderation) can help children learn social, language, and reading skills. | For children 2 to 5 years of age,<br>• Limit screen use to no more than 1 hour per day.<br>• Find other activities for your children to do that are healthy for their bodies and minds.<br>• Choose media that is interactive, non-violent, educational, and prosocial.<br>• Co-view or co-play with your children. |

TECHNOLOGY IS MORE EFFECTIVE WHEN USED TOGETHER

Engage Communicate Learn Create

## ONLINE SAFETY TIPS

**In the world of technology, there are so many possibilities. It is difficult to pinpoint every risky behavior, which is why we stress the importance of parents regularly checking in with their kids and monitoring their devices. The more comfortable you are with their devices the easier it will be for you to know what to look for. Here is a brief overview of ways to keep your children safer online.**

- Discuss internet safety and develop an online safety plan with children before they engage in online activity.
- Establish clear guidelines, teach children to spot red flags, and encourage children to have open communication with you.
- Supervise young children's use of the internet, including periodically checking their profiles and posts. Keep electronic devices in open, common areas of the home and consider setting time limits for their use.
- Review games, apps, and social media sites before they are downloaded or used by children. Pay particular attention to apps and sites that feature end-to-end encryption, direct messaging, video chats, file uploads, and user anonymity, which are frequently relied upon by online child predators.

- Adjust privacy settings and use parental controls for online games, apps, social media sites, and electronic devices.
- Tell children to avoid sharing personal information, photos, and videos online in public forums or with people they do not know in real life. Explain to your children that images posted online will be permanently on the internet.
- Teach children about body safety and boundaries, including the importance of saying 'no' to inappropriate requests both in the physical world and the virtual world.
- Be alert to potential signs of abuse, including changes in children's use of electronic devices, attempts to conceal online activity, withdrawn behavior, angry outbursts, anxiety, and depression.
- Encourage children to tell a parent, guardian, or other trusted adult if anyone asks them to engage in sexual activity or other inappropriate behavior.
- Immediately report suspected online enticement or sexual exploitation of a child by calling 911, contacting the FBI at tips.fbi.gov, or filing a report with the National Center for Missing & Exploited Children (NCMEC) at 1-800-843-5678 or report.cybertip.org.

Source: DOJ

## Teach your child to:

- ·Be as anonymous as possible
- Use privacy settings
- Think before they post
- Avoid in-person meetings
- Be honest about their age
- Remember social networking sites are public spaces
- Avoid posting anything that could embarrass them later or expose them to danger
- Remember that people aren't always who they say they are
- Check comments regularly
- Avoid inappropriate content and behavior, and, if encountered, report it to the social networking site

Source: InternetSafety101.org

## CYBERBULLING

An important topic to discuss regarding online safety is cyberbullying. Cyberbullying is the use of technology to harass, threaten, embarrass, or target another person. The effects of cyberbullying can be very serious, and it is not to be something that is taken lightly. There can also be serious consequences for those engaging in such behavior. Talk to your kids about cyberbullying to ensure they are not a victim, instigator, or bystander.

### Examples of cyberbullying:

- Posting comments or rumors about someone online that are mean, hurtful, or embarrassing.
- Threatening to hurt someone or telling them to kill themselves.
- Posting a mean or hurtful picture or video.
- Pretending to be someone else online in order to solicit or post personal or false information about someone else.
- Posting mean or hateful names, comments, or content about any race, religion, ethnicity, or other personal characteristics online.
- Creating a mean or hurtful webpage about someone.

## WARNING SIGNS A CHILD IS BEING CYBERBULLIED OR IS CYBERBULLYING OTHERS

Many of the warning signs that cyberbullying is occurring happen around a child's use of their  device. Some of the warning signs that a child may be involved in cyberbullying are:

- Noticeable increases or decreases in device use, including texting.
- A child exhibits emotional responses (laughter, anger, upset) to what is happening on their device.
- A child hides their screen or device when others are near, and avoids discussion about what they are doing on their device.
- Social media accounts are shut down or new ones appear.
- A child starts to avoid social situations, even those that were enjoyed in the past.
- A child becomes withdrawn or depressed, or loses interest in people and activities.

## WHAT TO DO WHEN CYBERBULLYING HAPPENS

If you notice warning signs that a child may be involved in cyberbullying, take steps to investigate that child's digital behavior. Cyberbullying is a form of bullying, and adults should take the same approach to address it: support the child being bullied, address the bullying behavior of a participant, and show children that cyberbullying is taken seriously. Because cyberbullying happens online, responding to it requires different approaches. If you think that a child is involved in cyberbullying, there are several things you can do:

- Notice – Recognize if there has been a change in mood or behavior and explore what the cause might be. Try to determine if these changes happen around a child's use of their digital devices.
- Talk – Ask questions to learn what is happening, how it started, and who is involved.
- Document – Keep a record of what is happening and where. Take screenshots of harmful posts or content if possible. Most laws and policies note that bullying is a repeated behavior, so records help to document it.

- Report – Most social media platforms and schools have clear policies and reporting processes. If a classmate is cyberbullying, report it the school. You can also contact app or social media platforms to report offensive content and have it removed. If a child has received physical threats, or if a potential crime or illegal behavior is occurring, report it to the police.
- Support – Peers, mentors, and trusted adults can sometimes intervene publicly to positively influence a situation where negative or hurtful content posts about a child. Public Intervention can include posting positive comments about the person targeted with bullying to try to shift the conversation in a positive direction. It can also help to reach out to the child who is bullying and the target of the bullying to express your concern. If possible, try to determine if more professional support is needed for those involved, such as speaking with a guidance counselor or mental health professional.

Source: stopbullying.gov

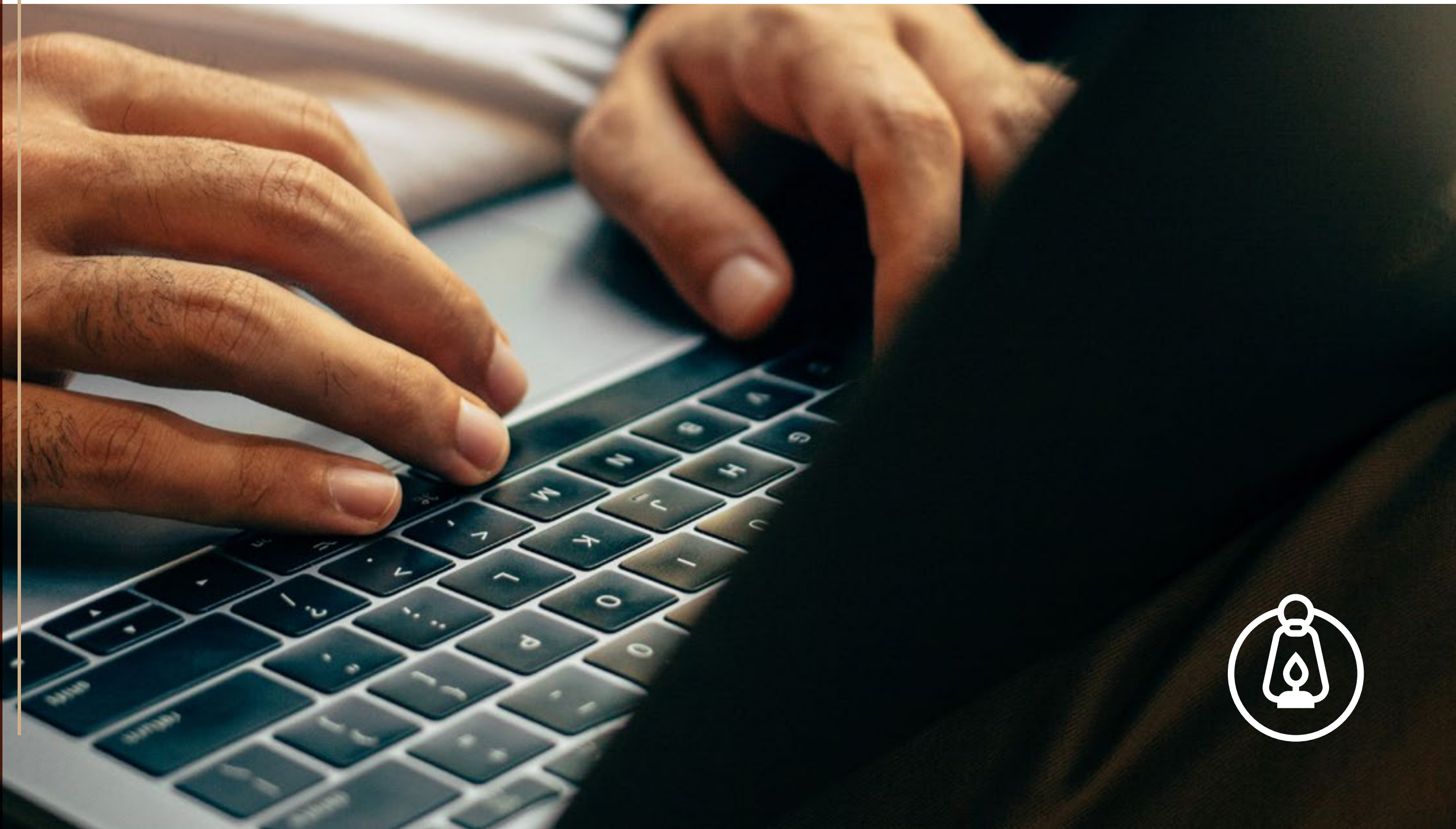
*Cyber bullies can hide behind a mask of anonymity online and do not need direct physical access to their victims to do unimaginable harm.*

–Anna Maria Chavez

## PORNOGRAPHY

While it might seem intimidating or inappropriate to discuss unsafe images with your children, it is important to initiate the conversation before they are introduced to these types of images by someone else or stumble upon them on the internet.

Pornography is so much easier to access in this digital age than ever before--kids don't even have to seek it out, oftentimes they are introduced to it unintentionally. Pornography can be accessed anywhere, anytime. Nowadays children can encounter porn (intentionally or unintentionally) through websites, social media, chatrooms, messaging, gaming, spam, and other uses. There are many dangers of pornography including that it can lead to addiction, desensitizes them to sexual acts, normalizes sexual harm, promotes aggression towards women, shapes unsafe sexual practices, and more.



Talk to your kids about pornography:

- Define pornography so that the termniology is clear.
- Talk about good pictures vs bad pictures (see resource below).
- Set clear boundaries (can be referenced in your Family Media Value Guide) concerning viewing pornography on their devices.
- Establish a safe zone where your children can report any unsafe images or concerns to you immediately with the understanding that they will not get in trouble. If there is open communication and an established method of reporting dangerous material without repercussions they will be more likely to keep you involved.

Resources:
Good Pictures Bad Pictures: Porn-Proofing Today's Young Kids for kids ages 6 - 11
Good Pictures Bad Pictures Jr.: A Simple Plan to Protect Young Minds for kids ages 3-7

## CHILD SEXUAL ABUSE MATERIAL (CSAM):

It would be remiss of us to not address one of the biggest issues of online safety: child sexual abuse material. As defined by Thorn "Child sexual abuse material (legally known as child pornography) refers to any content that depicts sexually explicit activities involving a child. Visual depictions include photographs, videos, digital or computer generated images indistinguishable from an actual minor. These images and videos that involve the documentation of an actual crime scene are then circulated for personal consumption."

In recent years there has been an increase among minors in self-produced content and content stemming from online-enticement. You read that right: CSAM material can be produced by children through ignorance or coercion. According to the Department of Justice, " Federal law prohibits the production, distribution, importation, reception, or possession of any image of child pornography." For this reason, we want children and teens to understand that not only is it dangerous to take and share sexually explicit photos of themselves or others (minors), there can also be serious consequences of doing so.

Talk to your kids about:

- Appropriate vs inappropriate images on their devices. Iit is best to be direct when discussing what type of photos you do not want your children to take of themselves or others to ensure they understand the boundaries and expectations.

- Discuss peer pressure and what to do when someone requests something that makes them feel uncomfortable or unsure. Explain that it doesn't matter if it is a boyfriend/girlfriend, friend, or stranger-- they should never feel pressured or threatened to send a sexual image. Talk about what to do if this happens and come up with a strategy so they know you are in this together.

- Remind your child that once a photo is sent or posted it cannot be retracted-- there is always a digital footprint. Even apps like Snapchat which are intended to "disappear" after they are viewed do not fully disappear.

- It is illegal to send photos of a minor containing any form of nudity, even when these photos are self-produced.

- There is always a possibility that photos/videos/content sent to friends or boyfriends/girlfriends can be used against them by the recipient in the future. We touch on this in the "sextortion" section, but it is not uncommon for people to send/forward photos to people other than their intended viewer. This is another reason not to share private or revealing photos of yourself or others.

*The plague of pornography is swirling about us as never before. Pornography brings a vicious wake of immorality, broken homes, and broken lives. Pornography will sap spiritual strength to endure. Pornography is much like quicksand. You can become so easily trapped and overcome as soon as you step into it that you do not realize the severe danger. Most likely you will need assistance to get out of the quicksand of pornography. But how much better it is never to step into it. I plead with you to be careful and cautious.*

–Joseph B. Wirthlin

Unfortunately the internet is full of predators who prey on the vulnerable, and this leaves children most at risk. Online predators use many tactics to lure unsuspecting children including gaining their trust through flattery, compliments, showing interest in their hobbies and interests, and pretending to be someone they are not. It is imperative that we teach our children that not everyone is who they say they are online.

Predators will:

- Prey on teen's desire for romance, adventure, and sexual information
- Develop trust and secrecy: manipulate child by listening to and sympathizing with child's problems and insecurities
- Affirm feelings and choices of child
- Exploit natural sexual curiosities of child
- Ease inhibitions by gradually introducing sex into conversations or exposing them to pornography
- Flatter and compliment the child excessively, sends gifts, and invests time, money, and energy to groom child
- Develop an online relationship that is romantic, controlling, and upon which the child becomes dependent

- Drive a wedge between the child and his or her parents and friends
- Make promises of an exciting, stress-free life, tailored to the youth's desire
- Make threats, and often will use child pornography featuring their victims to blackmail them into silence

Source: InternetSafety101

## PRECURSORS/ WAYS PREDATORS MANIPULATE VICTIMS

### ONLINE ENTICEMENT-

Online Enticement involves an individual communicating with someone believed to be a child via the internet with the intent to commit a sexual offense or abduction. This is a broad category of online exploitation and includes sextortion, in which a child is being groomed to take sexually explicit images and/or ultimately meet face-to-face with someone for sexual purposes, or to engage in a sexual conversation online or, in some instances, to sell/trade the child's sexual images. This type of victimization takes place across every platform; social media, messaging apps, gaming platforms, etc.

Source: NCMEC/Netsmartz

### Red Flags:
### The most common tactics used to entice children include:

- Engaging in sexual conversation/role playing as a grooming method, rather than a goal.
- Asking the child for sexually explicit images of themselves or mutually sharing images.
- Developing a rapport through compliments, discussing shared interests or "liking" their online post, also known as grooming.
- Sending or offering sexually explicit images of themselves.
- Pretending to be younger.
- Offering an incentive such as a gift card, alcohol, drugs, lodging, transportation or food.

Source: NCMEC/Netsmartz

GROOMING-

Grooming is the precursor phase. Sexual grooming, or just "grooming", is a preparatory process in which a predator gradually gains a person's trust with the intent to exploit them. The victim is usually a child, teen, or vulnerable adult. The purpose of grooming is to manipulate the person into becoming a co-operating participant in their own abuse or exploitation, which reduces the likelihood of a disclosure and increases the likelihood that the victim will become attached and repeatedly return to the perpetrator.

Stages of grooming: targeting a victim, gaining trust and information, filling a need, isolation, abuse begins, maintaining control

Source: FightToEndExploitation.org

Video on keeping kids safe from grooming and manipulation: D2l.org

## 10 grooming behaviors every parent should recognize:

- Seeks out and pays extra special attention to a child
- Acts overly interested in the child
- Buys them gifts and or treats
- Touches or hugs them in front of trusted adults which makes the child think the touching is OK
- Finds out what your child's likes and interests are and then flatters the child by claiming to have the same likes and interests
- Pretends to be a good friend to the child, even "best friends" and acts as a sympathetic listener when child is upset
- Tries to find ways to be alone with the child
- Tells the child dirty jokes or shows them pornography
- Grooms parents to gain more access to the child such as offering to babysit
- Grooming happens online as well so be aware of your children's online activities

Source: ProtectYoungMinds.org

## SEXTORTION-

Sextortion takes on different forms, but at its core, it is the threat to expose sexual images in order to make a person do something. These threats come from both strangerst met online and once intimate romantic partners attempting to harass, embarrass, and control victims.

## Sextortion Stats:

- 1 in 4 victims were 13 or younger when threatened
- 2 in 3 victims were girls threatened before the age of 16

## Consequences of Sextortion:

- Sextortion causes serious harm: 1 in 4 victims saw a medical or mental health professional.
- 1 in 3 victims did not tell anyone, often because of shame, embarrassment, and self-blame.
- 1 in 8 victims move from their homes in fear for their safety

Source: Thorn

## LOVERBOY METHOD-

Loverboys are traffickers and procurers (often teenagers themselves) who operate via social media, leading unsuspecting minors to believe they are in love with them. Most cases occur in chat rooms and on social media chat rooms. In the beginning victims receive a lot of attention and gifts and are thereby lured into love. The Loverboy seeks to systematically create a relationship of dependency and purposefully tries to alienate his victim from their family and friends. As soon as such a relationship has been established, he takes further steps to lead his victim into prostitution, shoots sex films and lures the victim into committing crimes. His primary goal is to earn a fortune with the minors. Victims are typically between 12 and 18 years of age.

Source: Act212

## HOW TO REPORT ABUSE:

The Department of Justice website contains information on how to report violations for child pornography, child sex trafficking, child sexual abuse.

While technology evolves at a rapid rate, it can be difficult to keep up with all the advances. However, you want to ensure that every device (smartphone, tablet, laptop, etc.) your child uses is as safe as possible. Below you will find websites, software, and toolst to safeguard your devices.

## INSTRUCTIONAL GUIDES:

- **Common Sense Media** compiled a wide array of parental control solutions, from OS settings to monitoring apps to network hardware. Some of these include:
    - Blocking Websites
    - Filtering Content
    - Setting limits and monitoring kids
    - Tracking location
- **Pixel Privac**y compiled this resource titled “How To Keep Your Children Safe Online: The Ultimate Guide For The Non Techy Parent” that combines practical ways to encourage safe internet use along with parental control step-by-step instructions for things like:
    - Apps
    - Web/browser
    - Time
    - Privacy

## HELPFUL SOFTWARE:

- **Bark**- Bark helps families manage and protect their children's online lives. They monitor 30+ of the most popular apps and social media platforms, including text messaging and email, for signs of digital dangers. Their screen time management and web filtering tools help you set healthy limits around how and when your kids use their devices.

- **Covenant Eyes**- accountability app to keep porn off your devices

## HOW TO SECURE INDIVIDUAL DEVICES:

Apple iPhone
Apple Macbook
Apple TV
Chromebook
Chromecast
Kindle Fire
Nintendo 3DS
Nintendo Switch
Amazon Fire Stick
Playstation 4
Playstation 5
Xbox
Roku/Roku TV
Wireless Router
Smart TV
Netflix Parental Controls
Amazon Video Parental Controls
YouTube Parental Controls
Gaming Consoles

Alternative Source to Secure Phones:

InternetMatters.org

> *Oftentimes parents are influenced by their environment and certain trends, so it's really not surprising that raising a child is now is different than it was a few decades ago, especially when you look at all of the new technological advances we've seen since.*
>
> –Jessica Booth

# CONTINUED LEARNING

Be sure to join our email list for future updates. You can also find us on social media **@the.lantern.project** to stay in touch and get the latest tips, stats, and announcements.

THE
**LANTERN**
PROJECT