Office of the Hunterdon County Prosecutor

RENÉE M. ROBESON
PROSECUTOR

JOSEPH PARAVECCHIA
FIRST ASSISTANT PROSECUTOR

TIMOTHY J. DREW
CHIEF OF DETECTIVES

Justice Center, 2nd Floor
65 Park Avenue
PO Box 756
Flemington, NJ 08822-0756

Telephone 908-788-1129
Fax 908-806-4618
www.co.hunterdon.nj.us/prosecutor/

It's time for a smarter conversation about social media.

Whether we like it or not, social media plays an important role in our kids' lives. They socialize, experiment with their identities, exercise their voices, and learn about the world through photo and video sharing apps, instant messaging, and gaming chats.

We want to shield our children from harm when they are online, but when we let worries about keeping our kids safe dictate how we protect them, we can overlook teaching them the skills they need to navigate their online lives without our constant oversight.

- **Talk with your tween** about what it means to "Pause" before they post or hit send and why it matters.

- **Strategize.** What strategy would work best to help your child be more intentional or safe with their digital communications? Maybe for your tween it would work best for them to check in with you prior to posting or sending something? Developing an open communication line is key and can help both children and parents navigate the digital world.

- **Check In.** Speak with your child about what's new, how are kids talking/communicating online, is it secure/safe? Be open to the idea that you may need to help them come up with alternate ways to communicate with friends.

TikTok

What is TikTok?

TikTok is an app that allows people to view, create and share short videos with friends, family, or the entire world. Although used by lots of adults of all ages, the app is especially popular with teens and young adults, who enjoy using its tools to combine video, popular songs, and graphics into fun sketches, creative shorts and viral videos.

Is TikTok safe for kids?

As with any social media app, a positive experience on TikTok ultimately depends on how it is used. TikTok has **built-in safety and privacy features** that vary based on the user's age. For example, kids under 13 access a different app experience called TikTok for Younger Users, which offers a curated feed of age-appropriate content. Teens 13-15 have private accounts by default and can't live stream or send direct messages.

Are TikTok accounts public or private?

For people under 16, TikTok accounts are automatically set to private. For people over 16, TikTok accounts are automatically set to public, but everyone has the option to set their profiles — and any TikToks they create — to private.

What are TikTok challenges?

Activities, dances — really anything that can go viral and inspire others to imitate the idea and spread it further. Participating in challenges can make people feel part of the broader TikTok community — say, by learning the latest dance and sharing their version of it — but people should exercise caution when participating in challenges, especially ones that may require a special skill. Talk to your kids about **dangerous viral internet challenges** and the peer pressure to participate.

Parents ask: How can I keep my kids safe?

Start by talking with your teen about how they use TikTok. Make sure they understand that the videos and comments they post affect their or others' reputations and that they

should never post anything that jeopardizes their privacy and security. Make sure your teen knows how to block anyone who bullies, threatens, or harasses them, or if they don't want that person to see their content or comment on their videos.

TikTok offers **Family Pairing**, which allows parents and guardians to pair their TikTok account with their teenager's account to guide their teen's use of the app. Parents can decide whether their child can search for content, users, songs or hashtags, set daily screen time (40 to 120 minutes a day), set the account to public or private, limit who can comment on their videos, turn off direct messaging and enable Restricted Mode, which "can limit content that may not be appropriate for some audiences."

More ways to stay safe:

Moderation and abuse reporting. To enforce its **Community Guidelines**, TikTok uses a combination of policies and human- and machine-based moderation practices to handle content that may violate its guidelines. To report a comment: Press and hold on the comment and select Report. To report an inappropriate video, tap the Share arrow and choose Report. Report a profile by going to the profile, tapping on the three dots and selecting Report.

Passwords and other personal information. Talk with your kids about the importance of keeping passwords and other personal information private. Friends can become ex-friends and use their account in mean or inappropriate ways. You'll find password tips at **ConnectSafely.org/passwords**.

Time management and life balance. Whether it's TikTok or any other app, teens (and adults too) need to put down their phones and interact with others in person. No app should ever keep you or your teen from getting exercise, doing chores, work or anything else that keeps us healthy, happy, and productive. If you need a nudge, use the time management features in the TikTok app or Apple and Android phones.

A note about parental controls. Parental controls have their place,but sometimes conversations can accomplish even more. For general advice on parental controls, including suggestions for talking about them with your kids, visit **ConnectSafely.org/controls**. Parents can enable Restricted Mode to limit the appearance of content that may not be appropriate for all ages.

Snapchat

Tips for you and your kids:

- **Manage your settings.** Snapchat's privacy settings are important to understand. The default "My Friends" setting only allows users to send and receive media from users they have added to their friends list. We recommend that any minor using Snapchat continues to use this setting. For more help with this, visit https://support.snapchat.com/a/privacy-settings.

- **Personal information.** Remind your kids to be careful about sharing any personally identifiable information. Financial and medical information should never be shared. Phone numbers and home addresses should only be shared, as necessary, with friends or family who you trust with that information.

- **Saving Snaps.** Even though Snaps aren't saved by default, it's always possible for the creator to save a Snap before sending it or for a viewer to take a screenshot. One can even take a picture of the screen with another camera or use other tools to save a copy. So it's important to remind kids to never send Snaps that are illegal, could get them in trouble now or in the future, or would be embarrassing if seen by people like grandparents or college admissions officers or future employers.

- **Protect passwords and set up two-factor authentication.** Like all services, make sure your kids have a strong and unique password that they don't share with anyone. If someone has their password, it's possible for them to impersonate them or compromise their account. For more on this, visit ConnectSafely.org/Passwords.

- **Device-level controls.** Android and iOS operating systems offer parental controls for mobile devices. Use these to manage your child's phone usage actively. For general advice on parental controls visit ConnectSafely.org/Controls.

- **Keeping it real.** Snapchat is a service designed for "real life" friends, but there are still ways for your kids to find people they don't know (such as finding their Snapchat username on other services). Remind your kids that it's best to only friend people they know in real life and it's not safe to meet-up with a person they meet online.

- **Location considerations.** Teach your kids to be thoughtful about sharing their location. We recommend teens stay in Ghost Mode with everyone but close family members and a few trusted friends.

- **Bullying.** Bullying violates Snapchat's Community Guidelines and is not tolerated on the platform. Make sure to talk with your kids about why bullying is wrong. Also, remind them to speak to you or any other trusted adult if they are ever on the receiving end of bullying or unwanted content. For more advice on talking to your kids about cyberbullying, visit connectsafely.org/cyberbullying.

- **Nudity.** Aside from violating Snapchat's community standards, teens need to know that exchanging nude or sexually explicit images of anyone under 18, including themselves, can be a serious crime. For more on this, see connectsafely.org/tips-for-dealing-with-teen-sexting/.

What to do about harassment or unwanted Snaps?

If your teen's settings are set to "My Friends" but they are still receiving abusive Snaps from another user, they should block the user and report them to Snapchat's Safety team.

- **Block.** Snapchat allows users to block Friends from sending them Snaps or Chats or viewing their Story. Press and hold on to the person's name and tap More and then Block.
- **Report abuse.** Press and hold on the Snap and tap the flag icon. If anyone receives inappropriate photos or someone's harassing him or her, contact Snapchat's Safety team by going to support.snapchat.com/en-US/ca/policies-and-safety and navigating to the "Report a Safety Concern" tab in the menu. If you encounter anything that appears to be illegal or dangerous, or if you have reason to believe someone is at risk of harm or self-harm, immediately contact local law enforcement.

ConnectSafely.org is a good resource to pull from if you are looking for information and tips.

https://internetsafety101.org/
https://www.icactaskforce.org/internetsafety
https://www.netsmartzkids.org/

Thank You

Bryan Hanley
Detective, Deputy Commander Narcotics Task Force / Forensic Services Unit, ICAC Task Force

Hunterdon County Prosecutor's Office
65 Park Avenue
P.O. Box 756
Flemington, NJ 08822
Phone: 908-788-1129
Fax: 908-788-1460

Internet Safety at Home

NetSmartz®

As adults and children alike have turned to digital tools for school, work, and socialization, **online safety matters now more than ever.**

Here are **five tips** for keeping kids safer online, adapted to fit the current "safer at home" environment.

Tip 1: Keep the Ground Rules

Even if our online habits have changed significantly, you can still set boundaries that work for your family and schedule. Involving children in setting these rules may help them stick to the guidelines.

Consider:

- Distance learning tasks **before** social media or gaming
- **No devices** during meals
- At least ___ **minutes** of non-electronic activities per day
- **"Digital curfew":** no devices after a certain hour

Tip 2: Modify How You Monitor

Even the strictest monitoring programs and content blockers can't ensure that children are totally protected online. The best tools for keeping kids safe are time, attention and active conversation about digital behaviors.

Consider: Setting up **workstations** for children and teens that provide **quick visual access** to the screens for **easy check-ins** from parents/caretakers as they telework or complete household tasks.

Tip 3:

Engage with the Platforms

Take advantage of this time at home and online to get more familiar with the technology platforms your child likes to use. Taking a genuine interest in the games and platforms your child enjoys will help you better understand what your child is doing online.

Consider: If you're teleworking, **take a short break** to join your child on a round on the **game console,** or forward a funny **meme or video** you saw on one of the social media channels they use. It's a quick way to show you're willing and able to be **involved** in your child's online life.

Tip 4:

Chat IRL

Chat "in real life" with your children. With our social lives being conducted entirely online these days, it's important to have face-to-face discussions about how children and teens are maintaining healthy relationships online, and to give them opportunities to also talk about anything unhealthy or uncomfortable happening to them online.

Consider: Showing that you're willing to **listen and respond calmly,** even if what you hear is uncomfortable or troubling.

Tip 5:

Don't Take the Tech

Taking away internet access because a child has made a mistake online rarely solves the problem. Taking access away during a lockdown would likely do far more harm than good. Beyond affecting a child's ability to complete distance-learning tasks, it would all but completely isolate them from friends and other family; a support system that is essential right now. Find ways to give consequences that don't involve removing online access entirely.

Consider: If you must, **limit access** (shorter window for digital socializing, gaming, restricted use to certain public areas of the house, etc.) **rather than** removing it entirely.

NetSmartz®

For more resources visit MissingKids.org/NetSmartz

Copyright © 2020 National Center for Missing & Exploited Children. All rights reserved.

A program of the NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

PARENTS' GUIDE TO SMART PHONE SAFETY

SMART OR SCARY?

Smartphones are essentially little computers, so you might be a little worried when handing one over to your child. Take some time to understand the risks and implement a few safeguards so that you can help your child use smartphones safely.

THE RISKS

- **CYBERBULLYING**
  With the constant connectivity of smartphones, your child may be more susceptible to cyberbullying or have more opportunities to cyberbully others.
- **GEOLOCATION**
  A GPS-enabled smartphone can reveal your child's location through online posts and uploaded photos.
- **INAPPROPRIATE CONTENT**
  With smartphones, your child has mobile access to content you may consider inappropriate, such as pornography or violent videos.
- **SEXTING**
  Your child may use the Internet and social apps to send, receive, or forward revealing photos.
- **VIRUSES & MALWARE**
  Just like a computer, a smartphone is vulnerable to security attacks if your child accesses unsecured websites and apps.

5 WAYS TO BE SMARTER THAN THE SMARTPHONE!

1. **Be a parent and a resource.**
   Establish clear guidelines, including time limits and consequences for inappropriate behavior, but be open so your child will come to you with any problems.
2. **Set up smart security.**
   Smartphones today include a variety of security mechanisms including fingerprint scans, facial recognition and password locks. Enable these to protect access to the phone as well as apps with sensitive data.
3. **Update the operating system.**
   New versions often contain important security fixes.
4. **Approve apps before they are downloaded.**
   Make sure you understand their capabilities and approve their content.
5. **Understand location services.**
   GPS features are useful when using maps, but you'll want to disable location-tagging when your child posts anything online.

For more resources visit MissingKids.org/NetSmartz/Resources

Copyright © 2012-2019 National Center for Missing & Exploited Children. All rights reserved.

NetSmartz®

A program of the NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

SOCIAL MEDIA SAFETY FOR TEENS

THE FOLLOWING CHECKLIST CAN HELP YOU TAKE STEPS TO KEEP YOURSELF SAFER ONLINE.

- ○ **CHECK YOUR COMMENTS AND IMAGES.**
  Have you posted anything inappropriate or illegal, like threats, nudity, alcohol, or drugs?

- ○ **TALK TO YOUR FRIENDS ABOUT WHAT'S OK TO POST.**
  Agree that you won't post embarrassing or hurtful comments or images of each other. Be clear that you'll delete – or if needed, report – any posts that are inappropriate, illegal, threatening, or could get you in trouble.

- ○ **REVIEW YOUR ACCOUNT SETTINGS.**
  Always ask yourself – what is on my profile and who can see it?

- ○ **KNOW YOUR FRIENDS, CONTACTS, AND FOLLOWERS.**
  These are the people who can see, share, and comment on what you post so you want to be sure you can trust them. Block and report anyone who makes harassing, threatening, or inappropriate comments.

- ○ **KEEP AN EYE ON 3RD PARTY AND CONNECTED APPS.**
  Some of these will allow you to log into one app using account information from another. Be careful, as this may allow the company access to your profile information.

- ○ **DON'T FORGET MOBILE.**
  When you use mobile devices like smartphones and tablets to post something or check in, you could also be sharing your location. Check your settings to make sure you're only sharing what you want to.

- ○ **REPORT.**
  You have the right to be safe online. If anyone cyberbullies you, make a report to the website or app. If anyone shares or asks you to share sexual messages or images, make a report to CyberTipline.org.

A program of the

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

Copyright © 2014-2019 National Center for Missing & Exploited Children. All rights reserved.

NetSmartz®

For more resources visit **Missingkids.org/NetSmartz/Resources.**

Gaming Safely

NetSmartz®

Parental involvement is critical when it comes to helping children game more safely. Take an **active interest** in the games that your child plays and wants to buy; that means **doing a little research** on the game's rating, game-play style, content and age-appropriateness.

Know about the settings and capabilities for the equipment and systems your child uses. For example, many children enjoy gaming on a console as well as a cellphone or tablet. Many platforms have "cross-play" features where people can find and communicate with users across multiple platforms and devices.

Keep gaming consoles in an easy-to-supervise location and be aware of other places where your child may be accessing games, like a friend's house or community center.

Tell your child never to give out personal information while gaming. This includes talking about personal information that might be revealed in a screen name or gaming profile. Remind them never to agree to meet offline with someone they know exclusively through gaming.

Set rules about how long your child may play, what types of games are appropriate, and who else may participate. Use the parental controls when setting up the game system. Look for ways (like a PIN number) to prevent your child from changing the settings.

Have your child check with you before using a credit/debit card online. That means no auto-saving card details on the game console or device.

Check to see if the games your child plays have reporting features or moderators. Review these features with your child. Remember, you can also report inappropriate online interactions with children to **CyberTipline.org**

Start a Discussion with Your Child

- Would you show me how some of your **favorite games** are played? **Could we play together?**
- How do you **respond** if someone bothers you while you are gaming?
- How much do you let people **know about you** while gaming?
- **What kinds** of people do you game with?
- Do you feel **safe** while you are gaming online? **Why or why not?**

A program of the

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

For more resources, visit **MissingKids.org/NetSmartz**

Copyright © 2020 National Center for Missing & Exploited Children. All rights reserved.

PROTECTING YOUR KIDS ONLINE 2.0

CONNECT

Set some ground rules.
Establish clear guidelines like what types of sites kids can visit, apps they can download, and when they can have access to electronics. Consider "blackout" periods that require disconnection.

Research before you buy.
It's important to learn about a device's capabilities before you buy. Will it allow unknown people to communicate with my child? Will this allow children to make unchecked purchases?

Go beyond safeguards.
Installing monitoring software doesn't guarantee your child will be safe online. Time, attention and active conversation are the best tools to protect them.

REPORT!
If your kids are dealing with cyberbullies or potential online enticement, report it to the website, cell phone provider, law enforcement or **CyberTipline.org**

LEARN

Know the platforms.
Online enticement happens across all platforms, so be aware of the sites, games and apps your children frequent. Ask them to show you how they use them.

Be proactive.
Teach your kids to spot common tricks used by online offenders. In NCMEC CyberTipline reports, the most common tactics used to entice a child online were:

- Engaging the child in sexual conversation/roleplay as a grooming method.
- Directly asking the child for sexually explicit images of themselves, or offering to mutually exchange images.
- Developing a rapport with the child through compliments and other supportive behaviors such as "liking" their online posts.
- Sending unprompted sexually explicit images of themselves.
- Pretending to be younger.
- Offering incentives for explicit content.

Spot the Red Flags.
A child who is experiencing online enticement may be:

- Spending increasing time online.
- Getting upset when he or she is not allowed on their device.
- Taking extra steps to conceal what they are doing online.
- Receiving gifts from people you don't know.

ENGAGE

Talk about it!
Your kids might not tell you everything, but ask anyway. Regular conversations about safety can go a long way in increasing trust and communication.

Get involved.
Challenge them to a duel. If you have kids who like to play online games, ask if you can play, too. When you respect their interests, they're more likely to respect your rules.

Don't pull the plug.
Taking away internet access because they may have made mistakes online doesn't solve the problem. Talk to them about protecting themselves and respecting others online.

NetSmartz®

A program of the NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

For more resources, visit MissingKids.org/NetSmartz

Copyright © 2010-2019 National Center for Missing & Exploited Children. All rights reserved.

NetSmartz

Sextortion:

What Parents Should Know

You've likely heard of sexting – sharing and receiving sexually explicit messages and nude or partially nude images by text or through an app. Though sexting can be part of normal adolescent sexual development, there are also risks, particularly **sextortion.**

Sextortion: A type of blackmail used by offenders to acquire additional sexual content from the child, coerce them into engaging in sexual activity, or to obtain money from the child.

Who Are the Perpetrators?

Often, victims know their extorters. They are current or former romantic partners. They may hold an initial sexual image that was sent intentionally by the victim and are now using it to get more content; threatening to spread the picture to friends and family if the victim does not comply.

60% of the time, the blackmailer is known to the victim.

Other times, the offender was met online. This could be a lone-actor or a coordinated group of extorters who work together to target and elicit explicit content from their victims. This type of extorter may request additional content (often of an increasingly explicit nature) or money.

Copyright © 2020 National Center for Missing & Exploited Children. All rights reserved.

How Does it Happen?

Sextortion can happen at the hands of both **peers** and **unknown**, online offenders.

When It's an **Unknown** Offender

Approach

Offenders often approach a child on social media after using it to learn about the child's interests, friends, school, family, etc.

Move platforms

It is common for offenders to make initial contact with a victim on one platform, then ask them to move to a second or third platform, usually those with encrypted messaging systems in order to make tracking their crime more difficult.

Coerce

This includes using tactics like:

- Initially offering something of value such as money or drugs in exchange for a sexual image
- Pretending to work for a modeling agency
- Developing a false rapport with the child
- Secretly recording explicit videos/ messages during chats
- Threatening to physically assault the child or his/her family
- Using multiple identities to contact the child
- Pretending to be younger and/or a member of the opposite sex
- Hacking accounts to steal sexual images, or
- Threatening to commit suicide if no images are sent

VS

When It's Someone Known

Acquire the Image

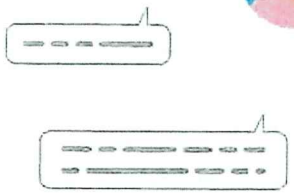
Often, the extorter is an ex-romantic partner who may have received the image deliberately from the victim while involved in a relationship.

Threaten

The extorter may use the threat of spreading the image to force the victim into staying in/ returning to the relationship after it has ended, or to acquire additional sexual content.

Persist

The harassment rarely stops if a victim complies with the extorter's demands.



Copyright © 2020 National Center for Missing & Exploited Children. All rights reserved.

What Can I Do About It?

Talk About Technology

Children should grow up expecting that their parents are a part of their digital lives. Regular check-ins about their online interactions should be the norm. Include children in setting rules and limits for their tech-time.

Talk About Sexuality and Relationships

Talking about your family's expectations and values regarding sex and relationships is an important first step. These conversations should happen regularly. Be sure to discuss the characteristics of healthy relationships, such as having and respecting boundaries and practicing consent. Explain that both pressuring someone and being pressured into sexual behaviors that are uncomfortable or unsafe are NOT OK. Similarly, help children understand that they should never forward sexts they may receive from others. Limiting the image's spread reduces the risk of it falling into dangerous hands.

What do you think you'd do if you got forwarded a nude?

I'm not sure...

It's simple. Delete it. It wasn't intended for you. Don't share it.

NetSmartz

For more resources, visit MissingKids.org/NetSmartz

Copyright © 2020 National Center for Missing & Exploited Children. All rights reserved.

A program of the NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

NetSmartz®

Uncomfortable Fact

Children are much more likely to be abducted or abused by **someone they know.**

Being a Trusted Adult

This reality can make it hard for children to understand what types of adult behaviors are inappropriate or dangerous. This is compounded when the abuser claims to love the child or is an authority the child has been told to respect.

BUT YOU CAN HELP! As a trusted adult, there are things you can do to demonstrate to children that you are a safe adult.

Respect children's bodies and boundaries

Trusted adults empower children to assert their boundaries and have control of their own bodies from a young age. This means talking about consent early. Children should understand that they can assert their own boundaries and that in turn they need to respect the boundaries of others. For example:

PRACTICE Boundaries

- *"Can I give you a hug?" "I don't really feel like a hug. How about a high five?"*
- *"Little brother, it doesn't look like your sister wants tickles right now- look at how she's frowning and looking down. Let's respect her space."*
- *"I noticed that you seemed uncomfortable when your coach gave you a hug today. Do you want to talk about it? It's OK to tell him you would prefer a high five."*

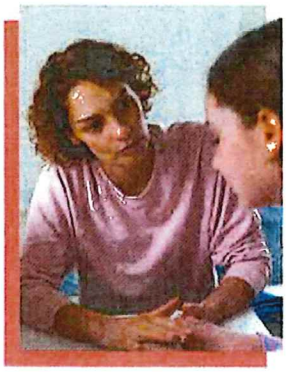
Listen and respond to children's concerns

When children approach you with safety concerns, it is important to take them seriously, even if they are seemingly small issues. By listening closely and treating the issue thoughtfully you help build confidence in children that they can trust you to help them when in trouble. This also helps empower them to be diligent about their own safety. Role playing can be helpful for children to help them practice being assertive about their boundaries.

PRACTICE Listening and Responding

"Mr. Jones, a girl on the playground grabbed my shirt and stretched it out."

"I'm sorry that happened. Are you OK? Try talking to the girl; let her know what she did and how it affected you. If it happens again, let me know and we will work it out together."



Be an informed resource

It's normal for children to use the internet to look for information about sex, development, and relationships. However, they may not be finding the best or most appropriate information this way. Talking to children openly about healthy relationships and having age appropriate conversations about sexual development will help reduce the risk that they are exposed to unhealthy or unrealistic information online.

PRACTICE Discussing Hard Topics

Abusers are emboldened by the taboo around talking to children about sex and sexual development. Get comfortable with the topics or terms that have made you uncomfortable in the past. Consider saying these words into a mirror, or rehearsing on your own something you want to later address with a child.

Model and explain to other adults

It can be hard to address the subject of child sexual abuse with family and friends, but avoiding these conversations is part of what allows it to continue. When practicing boundaries or listening and responding, be frank with the adults around you about why you are practicing these behaviors with the children in your life.

PRACTICE Modeling and Explaining

"My partner and I are trying to help the kids set their own physical boundaries; we're testing out handshakes versus hugs today. It's hard sometimes, but it's important to help keep them safe from abuse. Kids who have a good understanding of boundaries early on are better prepared to spot and report sexual abuse if it ever happened. We appreciate your support in this effort by not forcing the children to give a hug if they do not want to."

IT'S NOT EASY, BUT IT'S WORTH THE PRACTICE.

It is our shared responsibility to protect children.

For more resources, visit MissingKids.org/NetSmartz

Copyright © 2020 National Center for Missing & Exploited Children. All rights reserved.

NetSmartz®

A program of the NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN