PROTECTING YOUTH IN THE DIGITAL AGE

FBI Atlanta, GBI-GISAC, GEMA/HS, and GASROE collaborated to compile this reference for K-12 families with children who may have access to digital devices and potentially harmful content.

Youth and Digital Media

Smart phones, gaming consoles, tablets and other digital devices are part of everyday life for a growing number of American youth. With increased time interacting online comes increased risk. Youth can be exposed to hate-based digital content, violence, radicalization, or make themselves vulnerable to sexual exploitation and other online crimes.

Young people and caregivers should be aware that violent offenders can victimize children or teens in their own homes through the devices they use for gaming, homework, and communicating with friends. Youth are often initially contacted over a game, app, or social media account by predators or violent online groups. They deliberately target minor victims on publicly available messaging platforms to extort them into recording or live-streaming acts of self-harm and/or producing child sexual abuse material (CSAM). These groups operate under many names and continually evolve.

Criminals use intimidation, blackmail, and activities such as doxxing[1] and swatting[2] to manipulate their victims into producing CSAM and videos depicting animal cruelty and self-harm, including fansigning[3]. Participants gain notoriety and status within the groups based on shared evidence of victim manipulation seeking to escalate their number and degree of animal cruelty or self-harm inflicted.

COMMUNICATION

Talk to your children about being careful online and not sending photos, but to also let them know if they do, they can come to you if they find themselves victimized.

BOUNDARIES

Set boundaries and time limits on social media or digital devices. Encourage devices to be used in common areas or turned off or with caregivers overnight.

ONLINE GAMING

Most gaming consoles connect online and allow for private chats or harmful links to be shared. Be sure to review content warnings or know if kids are playing with verified screennames or strangers.

SETTINGS/CONTROLS

Use device- specific and/or service-provider parental and privacy controls. Set profiles to PRIVATE and know children's passwords. Know what devices

1 DOX also referred to as DOXXING is the action of obtaining and publishing personally identifiable information (PII) on the internet, usually for malicious intent.
2 SWAT also referred to as SWATTING is the action or practice of making a prank call to police or emergency services in an attempt bring about the dispatch of armed police officers such as a SWAT team to a particular address.
3 Fansigning is writing or cutting specific numbers, letters, symbols or names onto our body.

Indicators of Online Victimization

- Using DARK or INCOGNITO MODE to hide or delete browser history.
- Behavioral changes especially when receiving texts, emails, messages, or notifications.
- Changes in device usage such as sudden withdrawal from/avoidance of social media.
- Unexplained gifts, money, or digital devices like a new phone or tablet.
- Expressing sympathy or solidarity with criminals or perpetrators of violence.
- Isolating oneself from family/peers.
- Fresh cuts, scratches, scars (maybe in patterns or words), burns, or wounds.

Sextortion

The FBI is seeing an alarming increase in cases involving adults coercing children into producing sexual images and videos online, a crime called **SEXTORTION**. These predators have developed tactics enabling them to exploit children through their connected devices within their homes. According to FBI Atlanta[1]:

- Sextortion cases are up 700% since 2021.
- The average victim is between 10 and 17 years old but can be as young as seven years old, according to investigators.
- More boys fall victim to this crime than girls.
- In the last year, at least 12 Georgia kids died by suicide after falling for a sextortion scheme.

Take a moment to learn how **SEXTORTION** works.

1 https://www.atlantanewsfirst.com/2024/06/03/fbi-reports-700-increase-sextortion-schemes-targeting-teens-online/

Resources, and conversation guides are available at fbi.gov/StopSextortion.

By understanding the indicators of online victimization, parents and families can implement more effective strategies to protect young internet users. The below concepts are offered to improve children's experience safely interacting with digital content.

JULY 2024

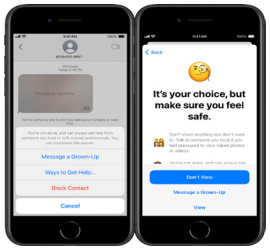
PROTECTING YOUTH IN THE DIGITAL AGE

Resources and Trainings

PROVIDER-SPECIFIC SETTINGS

Apple Families
https://www.apple.com/families/

Your child's Apple device will now prompt them with a pop-up message if it detects them sending or receiving potentially inappropriate content, such as nudity, in messages being sent or received if it is set up with Parental Controls and Communication Safety enabled.



- Powerful new privacy features released in June 2023 can also be disabled in the parent feature.
- Apple products "Screen Time" provide options to disable internet access at desired times "down time" or screen time limits specific to each app.

Android / Google Play Store
Families.google.com

- Creating a Google account for a child under 13, you can set up parental controls for them.
- Parental controls work on Android devices where your child is signed into their Google account. A parent in the Family Group needs to use their Google account to set controls for the youth account. You can set up "ask to buy" prompts for the App Store or manage other important settings.

Alternatives

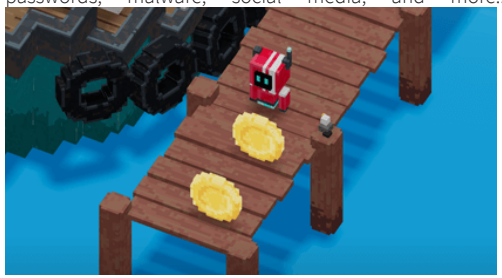
Many parents want a way their children can communicate with family and friends. Consider potential alternatives to smartphones for your kids. A variety of communication devices are available that enable calling or texting without full access to the internet. Research and consider some alternatives before getting your child a smart phone.

Information is being provided on accessing parental/safety controls for parents whose families own iPhone and Google/ Android devices. Parents whose families use other devices should contact the manufacturer to obtain information on accessing and enabling parental/safety controls. The FBI does not endorse any individual manufacturer or service provider.

SAFE ONLINE SURFING (SOS) INTERNET CHALLENGE

Federal Bureau of Investigation
https://sos.fbi.gov/en/

- Educational program geared toward 3rd – 8th grade teaching cyber safety and better digital citizenship in a fun and engaging way while addressing cyberbullying, passwords, malware, social media, and more...



(ABOVE): FBI-SOS CYBER SURF ISLAND GAME

CYBER BULLYING PREVENTION

Georgia Department of Education
https://www.gadoe.org/wholechild/Pages/Bullying-Prevention.aspx

The Georgia Department of Education offers a wealth of bullying prevention strategies and activities. The purpose of this Bullying Prevention Toolkit is to provide information to aid efforts to recognize and prevent bullying.

INTERNET CRIME COMPLAINTS CENTER (IC3)

Federal Bureau of Investigation
https://www.ic3.gov/

The Internet Crime Complaint Center, or IC3, is the Nation's central hub for reporting cyber crime. It is run by the FBI, the lead federal agency for investigating cyber crime. The website features two vital steps to protecting cyberspace and your own online security.

- First, if you believe you have fallen victim to cyber crime, file a complaint or report. Your information helps the FBI and its partners bring cybercriminals to justice.
- Second, get educated about the latest and most harmful cyber threats and scams. This will empower families to better protect themselves at home, school, or work.

NETSMARTZ FOR KIDS

National Center for Missing & Exploited Children (NCMEC)
https://www.missingkids.org/netsmartz/resources

- Since 1998, NCMEC has operated the CyberTipline, a place where the public and electronic service providers can report suspected online and offline child sexual exploitation. The millions of reports made each year uniquely situate NCMEC to identify trends and create prevention resources to address the evolving needs of youth online. NetSmartz is NCMEC's online safety education program. It provides age-appropriate videos and activities to help teach children to be safer online with the goal of helping children to become more aware of potential online risks and empowering them to help prevent victimization by making safer choices on- and offline.

The National Center for Missing and Exploited Children provides a free service known as Take It Down, which helps minor victims (even if they are now an adult who was victimized as a minor) remove or stop the online sharing of nude, or sexually explicit content taken while under 18 years old.

For more information, visit https://takeitdown.ncmec.org.

Source: IC3.gov

If you believe you are the victim of a crime using these types of sextortion or online tactics, retain all information regarding the incident (e.g., usernames, email addresses, websites or names of platforms used for communication, photos, videos, etc.) and immediately report it to your local police department. Other resources include:

- **FBI's Internet Crime Complaint Center at www.ic3.gov**
- **FBI Field Office (www.fbi.gov/contact-us/field-offices) or call 1-800-CALL-FBI (225-5324)**
- **National Center for Missing and Exploited Children (1-800-THE LOST or www.cybertipline.org)**

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN CYBER TIPLINE
www.cybertipline.com
1-800-843-5678