

# Online Safety Guidance and Resources for K-12 Schools

Thursday, February 24, 2022

SchoolSafety.gov



NATIONAL CENTER FOR  
**MISSING &  
EXPLOITED**  
CHILDREN®



# Webinar Agenda

- Webinar Objectives
- Speaker Introductions
- C3
  - Online Exploitation
  - Suggestions for Communities
  - Project iGuardian
- NCMEC
  - NetSmartz
  - NCMEC Connect
  - Resources for Survivors and Families
- SchoolSafety.gov
  - Grants Tool
  - CISA K-12 Suite
  - Additional Resources
- Q & A



SchoolSafety.gov



# Webinar Objectives

1. Provide an overview of how to foster digital ecosystems that are safe and secure for students and protect children from crimes of victimization.
2. Promote online safety practices and improve digital literacy and critical thinking skills to help reduce certain risk factors among youth.



# Featured Speakers



## Dianna Ford

Section Chief  
Child Exploitation Investigations Unit (CEIU)  
Victim Identification Program  
Cyber Crimes Center (C3)



## Susan Kennedy

Senior Program Manager  
Outreach and Prevention  
National Center for Missing & Exploited Children

SchoolSafety.gov

## Ryan Streeter

Program Manager – Product Branch  
School Safety Task Force  
Cybersecurity and Infrastructure Security Agency  
Department of Homeland Security

SchoolSafety.gov







# HSI

## Homeland Security Investigations

Child Exploitation  
Investigations Unit

Cyber Crimes Center





## Child Exploitation Investigations Unit (CEIU)

Supports the agency's international and domestic investigations of online child sexual exploitation to:

- Identify and rescue child victims
- Identify and apprehend the offenders
- Determine the location of abuse



**1,177**

**Children rescued from sexual exploitation in FY 2021**



**3,776**

**Criminal arrests in FY21**



# **What Law Enforcement wants you to know about child exploitation**





## Who are the victims?

Kids of all ages, races and backgrounds

## Kids are

- Inherently trusting
- Curious
- Unable to see long term consequences
- Able to be intimidated/coerced by adults
- In your community



# Who are the Offenders?

- People with access to children
- No one size fits all
- Males *and* Females
- Criminal Arrests and Convictions have included:
  - Priests/ministers
  - Volunteers
  - Doctors
  - Coaches
  - Teachers





# How do offenders reach out?

- Develop a positive rapport with the child
- Pretend to be younger (often when registering online accounts) – they know the same lingo
- Engage a child in sexual conversation/role-play as a grooming method
- Send sexually explicit images of themselves and ask children to reciprocate in the exchange of images
- Offer something other than an image in exchange
  - for example: a financial incentive / gifts
- In addition, offenders use a variety uncommon methods
  - pretend to be a different gender
  - modeling agent
  - using a fake/stolen account
  - recording or capturing images of child without authorization

# Online Perceptions & Personas

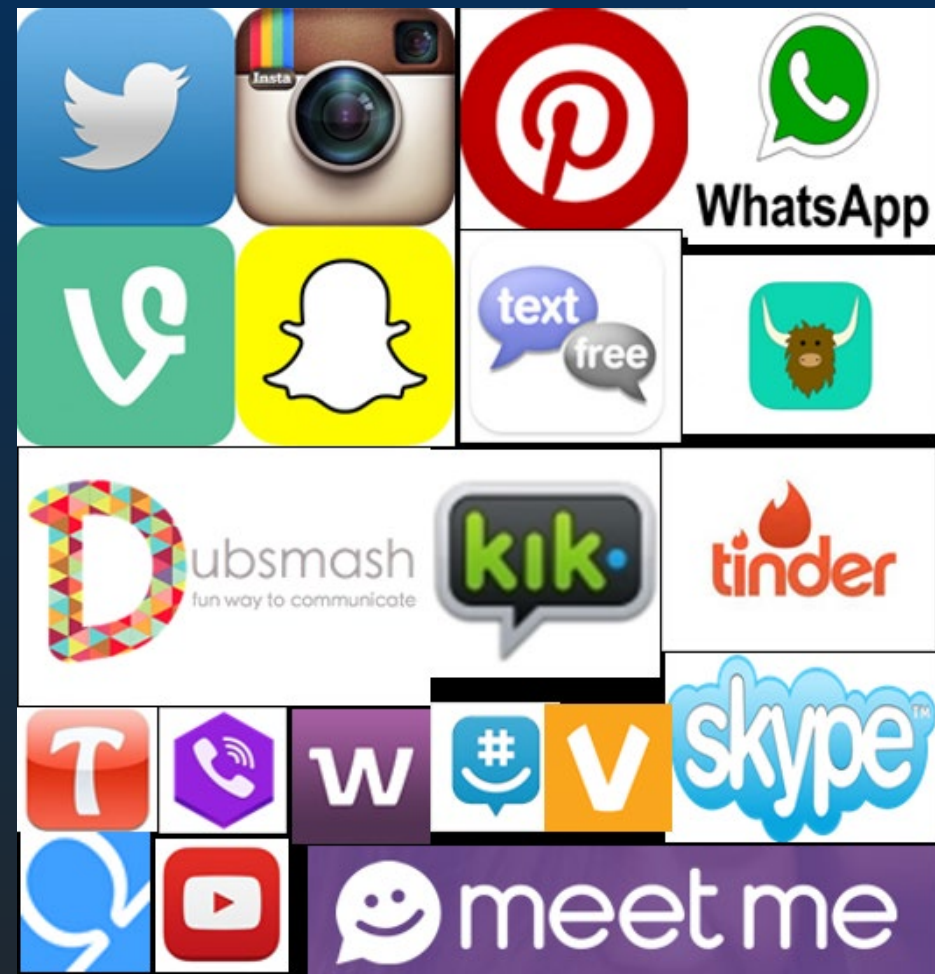






# Let's Talk Apps!

(there's so many!)



# Take Control of Your Children's Apps

- DOWNLOAD THE APP YOURSELF & BE THEIR FRIEND!
- FAMILIARIZE YOURSELF WITH THE APP'S USES
- SECURE PRIVACY & CONTROL WITHIN THE APP'S SETTINGS

Privacy Settings

Contact Settings are locked because Account Restrictions (under [Security](#) page) is enabled

**Contact Settings**

Off

Who can message me?

No one

Who can chat with me in app?

No one

Who can chat with me in game?

No one

Who can find me by my phone number?

No one



**ROBLOX**

Roblox Support > Parents, Safety, and Moderation > Safety

Search our articles

Articles in this section

## How can I see what my child is doing on Roblox?

Roblox has several ways to monitor account activity. While logged in, you can view the following histories from their related sections:

- Direct and small group chat (**Chat** feature found in the lower right corner of the apps). There you can see individual chat histories. This feature is limited to Friends, and Friends of Friends.
- Private message history (**Messages**)
- Friends and Followers (**Friends**)
- Virtual item purchase and trade history (**My Transactions** and **Trades**, browser only)
- Creations such as experiences, items, sounds, ads...etc (**Create**, browser only)
- Recently played experiences (**Home**, **Keep Playing** or **My Recent**)

If you can't log in, try these steps for [recovering your child's password](#).

[Need more help? Contact support here.](#)

Was this article helpful?

Yes No

[en.help.roblox.com](#)

<https://corp.roblox.com/parents/>

<https://en.help.roblox.com>



## Suggestions for Communities

- **Believe and listen to Children**
- **Be a trusted authority figure**
- **Be present with the kids-ask questions about what they are using online**
- **Join in their games and ask questions about who they are playing with**
- **Understand that revictimization happens when images have been uploaded online**
- **No one is immune**
- **There are families in your community who are dealing with exploitation of their children**
- **Train your staff, parents, and children on how to “Keep Kids Safer Online”**
  - Don't be afraid to start the conversation with a child – pay attention to changes in behavior and conversations. Be the adult and reach out!
- **Teach kids about good online habits:**
  - strong passwords,
  - keeping private things private,
  - turning off location information,
  - only socialize online with someone they've met in person and know,
  - don't send pictures to anyone or webcam with anyone, and
  - Never keep a secret – it's ok to discuss things with children and it's our responsibility to allow children to feel comfortable to discuss things with us.





## Overview of Project iGuardian

Keeping kids, teens, and parents safe from online predators through education and awareness

- Field offices offer presentations to area schools, churches, organizations, and children
- More than 58k children, parents, and educators were reached through Project iGuardian in 2021
- Developed in partnership with the National Center for Missing and Exploited Children's NetSmartz
- <https://www.ice.gov/topics/iGuardians>

## REPORT TO LAW ENFORCEMENT

## HOMELAND SECURITY INVESTIGATIONS



- To report suspicious activity or instances of child sexual exploitation, contact your local law enforcement agency.
- Tips can also be submitted online at <https://www.ice.gov/tipline>, by phone at 866-DHS-2-ICE or by contacting your local HSI office.
- For iGuardian presentations or follow-up questions, email [iGuardian@ice.dhs.gov](mailto:iGuardian@ice.dhs.gov).





Protecting the Homeland  
with **Honor, Service, and  
Integrity**

Q & A



# Online Safety Resources

Susan Kennedy

Senior Program Manager, Outreach & Prevention



NATIONAL CENTER FOR  
**MISSING &  
EXPLOITED**  
CHILDREN®



# OUR MISSION

**Find Missing Children**

**Reduce Child Sexual Exploitation**

**Prevent Future Victimization**

**Hope is why we're here.**



# Internet Safety



Connect



Learn



Engage

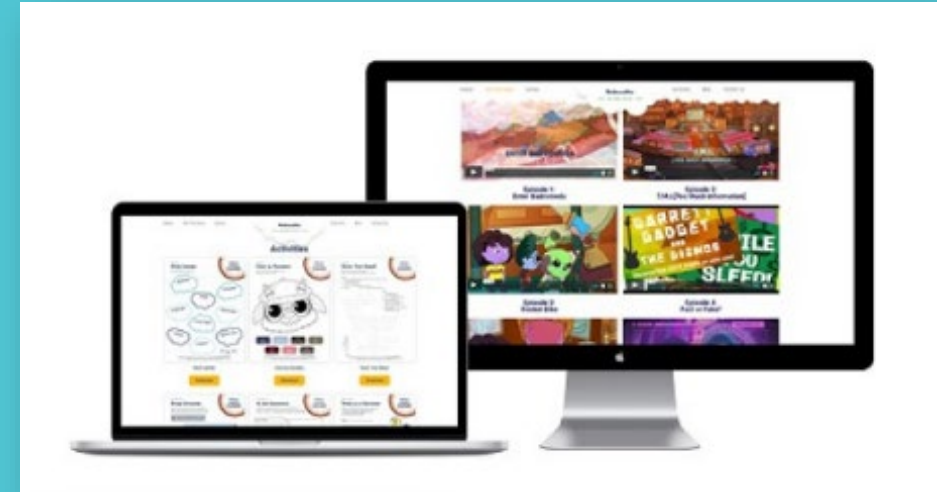
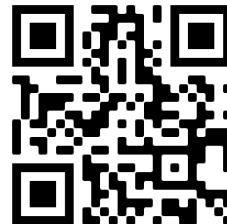
# NetSmartz®

Online safety program for children and families in grades K-12.

**Empower** children to take an active role in solving problems safely

**Engage** children and adults in two-way conversations about safety and risky behaviors

**Encourage** children to report unsafe behaviors or victimization



**NetSmartz®**

## Internet Safety at Home

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.

# Prevention Education & Community Outreach Tools

---

Free, interactive

Age-appropriate

Data-informed

Customizable

Point-in-time delivery

Training & technical assistance

Spanish-language materials  
available



# NetSmartz®

## With Younger Children

- Netiquette
- Looking at inappropriate content
- Pop-ups/passwords
- Not trusting everyone you meet online

## With Older Children and Teens

- Cyberbullying
- Sexting
- Posting personal/inappropriate content
- Meeting offline





## More Resources from **NetSmartz®**



### Activity Guides

From discussion tools to classroom lessons, these resources supplement NetSmartz video content and let students practice safety skills.



### Online Games

Interactive games that help children review online safety issues in fun and unique ways.



### Peer Education & Leadership Kits

Project-based learning opportunities for older students to teach younger students about digital citizenship and safety.



### NetSmartzKids.org

A safe site for kids! Watch "Into the Cloud" and classic NetSmartz videos, play games, read e-books and more, in a child-safe environment.



### Presentations

Scripted PowerPoint® presentations describing the main online safety issues and how to address them.



### Tip Sheets

Reference guides to remind parents and children about ways they can stay safer online.



### Videos

Animated and live-action videos, including the new web series "Into the Cloud", that show students how to apply important safety skills to on- and offline life.



### MissingKids.org/NetSmartz

Adults can learn more about the issues facing children online and access tools to help keep kids safer at MissingKids.org.



# Your Photo Fate





# Your Photo Fate – Discussion Questions

## Choices

- What was the very first choice made in the video?
- What were other decisions made in the video?

## Consequences

- What were the consequences for the boy who asked for the nude image?
- What were the consequences for the girl who sent the nude image?

## Healthy Relationships

- Should one person pressure the other to do something they are not comfortable doing?
- What would you tell a friend who was thinking about:
  - requesting a nude image from someone else?
  - sending a nude image to a significant other?



# Into the Cloud: Season 2, Episode 2 “The Picture”

---



# Into the Cloud Episode Discussion Guides



## DISCUSSION STARTERS

For grades K-2:

- Why did Zion go to Harold to talk about his problem? Who would you go to if you had a problem like Zion's?
- What is Zion's plan for getting the picture off the internet? What could you do in real life?

For grades 3-5

- If the user who took a screen capture of Zion had simply asked for a picture, should Zion have sent them one?
- If someone you didn't recognize sent you an inappropriate picture, what would you do?
- If someone you knew from school or a sport sent you an inappropriate picture, what would you do?



# | CONNECT



On-demand trainings, resources and best practices related to missing and exploited children including prevention

- Teaching Online Safety
- Child Safety Resources
- “Parent Connect” webinar series

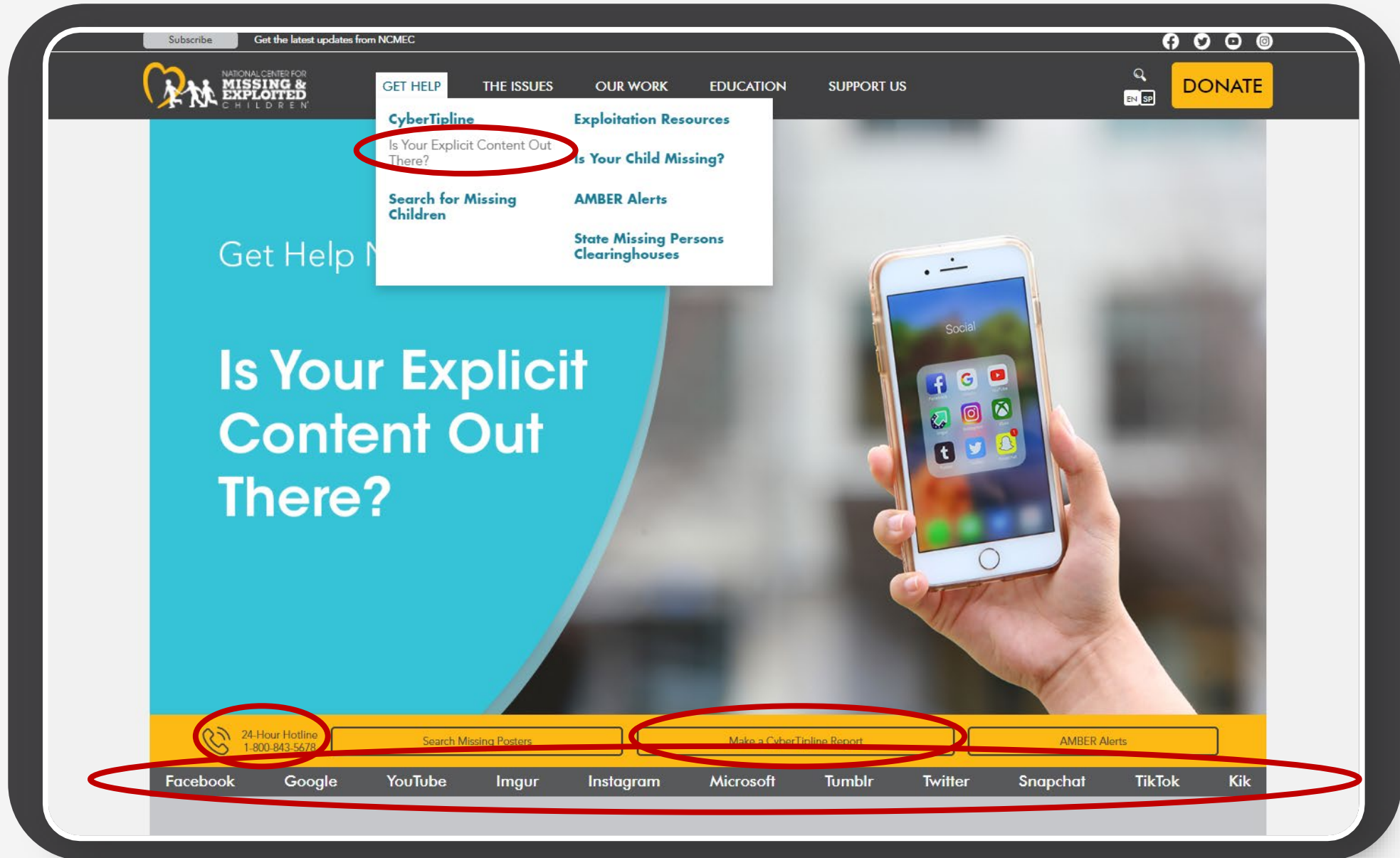


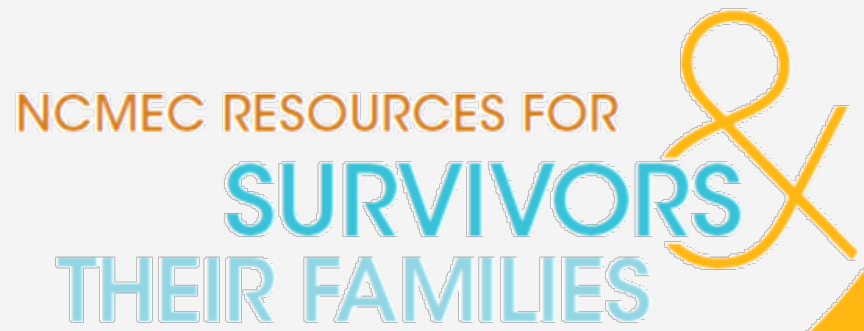
[connect.missingkids.org](https://connect.missingkids.org)

Training for  
**Professionals** | NCMEC CONNECT



# Help Removing Sexually Explicit Content





- Crisis Intervention
- Peer support network
- Mental health & community support referrals
- Reunification assistance
- Long-term emotional support
- Prevention strategies
- Legal referrals

**All services are FREE. Families do not have to have an active case to be eligible.**

[GetHelp@ncmec.org](mailto:GetHelp@ncmec.org)



**For more resources:**  
**MissingKids.org**  
**Outreach@NCMEC.org**



@MissingKids

**Copyright © 2021 National Center for Missing & Exploited Children. All rights reserved.**

This project was supported by Grant No. 15PJDP-21-GK-00998-MECP awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this program\* are those of the author(s) and do not necessarily reflect those of the Department of Justice.

For complete copyright and grant information, visit [MissingKids.org/Legal](https://MissingKids.org/Legal)



# SCHOOLSAFETY.GOV RESOURCES



33

SchoolSafety.gov



# Grants Finder Tool | SchoolSafety.gov



New tool that features Federally available **school safety-related grant opportunities** in one centralized location.

Designed to help schools determine **eligibility** and **applicability** of grant programs for their specific needs, challenges, and characteristics.

Option to **take quiz**, **select pre-populated lists**, or **filter grants** by specific criteria such as school safety topic, funding agency, application level of effort and deadline, and intended audience.

# Additional Resources

### Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center

CYBER SAFETY FOR SCHOOLS FACT SHEET


#### Cyber Safety Considerations for K-12 Schools and School Districts

The Internet allows for access to information 24 hours a day, 7 days a week. For schools (public and nonpublic), online capabilities not only create entrée to a vast amount of resources but also facilitate distance learning and collaboration between classes and students in different locations.<sup>1</sup> Along with the benefits the Internet brings, however, come costs such as new threats to students. Recent news articles provide examples of these threats: One man extorted sexually explicit images from minors using social media,<sup>2</sup> and instances of cyberbullying have reportedly soared in New York City schools.<sup>3</sup> These incidents can lead to depression and anxiety, health complaints, and decreased academic achievement by students.<sup>4</sup>

Some protections for children online are provided by Federal law and regulations, such as the Children's Internet Protection Act (CIPA).<sup>5</sup> CIPA aims to protect children from obscene or harmful content on the Internet. Schools or libraries that are eligible to receive discounts for telecommunications, Internet access, or internal connections through the E-rate program (Universal Service Program for Schools and Libraries) must certify they have an Internet safety policy that blocks or filters access to pictures that are obscene, child pornography, or harmful to minors.

While CIPA may help prevent students from accessing inappropriate content on the Internet, this will not protect students from the full range of online threats. To help address these, information is provided below on the most common online threats facing students and what schools can do before, during, and after an incident.

<sup>1</sup> School refers to all types, including private and public, and all grade levels for the purposes of this fact sheet.



REMS  
Readiness and Emergency Management for Schools  
Technical Assistance Center  
<http://remstac.org>

If you have questions or need additional assistance, please contact the REMS TA Center at 1 (855) 781-7367 or via e-mail at [info@remstacenter.org](mailto:info@remstacenter.org)

## Cyber Safety Considerations for K-12 Schools and School Districts (Dept. of Education)

### Technology and Youth: Protecting your Child from Electronic Aggression

Tip Sheet

Technology and youth seem destined for each other. They are both young, fast paced, and ever changing. In the last 20 years there has been an explosion in new technology. This new technology has been eagerly embraced by young people and has led to expanding knowledge, social networks, and vocabulary that includes instant messaging ("IMing"), blogging, and text messaging.


**Electronic Aggression is any type of harassment or bullying that occurs through e-mail, a chat room, instant messaging, a website (including blogs), or text messaging.**

New technology has many potential benefits for youth. With the help of new technology, young people can interact with others across the United States and throughout the world on a regular basis. Social networking sites like Facebook and MySpace also allow youth to develop new relationships with others, some of whom they have never even met in person. New technology also provides opportunities to make rewarding social connections for those youth who have difficulty developing friendships in traditional social settings or because of limited contact with same-aged peers. In addition, regular Internet access allows teens and pre-teens to quickly increase their knowledge on a wide variety of topics.


However, the recent explosion in technology does not come without possible risks. Youth can use electronic media to embarrass, harass, or threaten their peers. Increasing numbers of adolescents are becoming victims of this new form of violence—electronic aggression. Research suggests that 9% to 35% of young people report being victims of this type of violence. Like traditional forms of youth violence, electronic aggression is associated with emotional distress and conduct problems at school.

**Examples of Electronic Aggression**

- Disclosing someone else's personal information in a public area (e.g., website) in order to cause embarrassment.
- Posting rumors or lies about someone in a public area (e.g., discussion board).
- Distributing embarrassing pictures of someone by posting them in a public area (e.g., website) or sending them via e-mail.
- Assuming another person's electronic identity to post or send messages about others with the intent of causing the other person harm.
- Sending mean, embarrassing, or threatening text messages, instant messages, or e-mails.



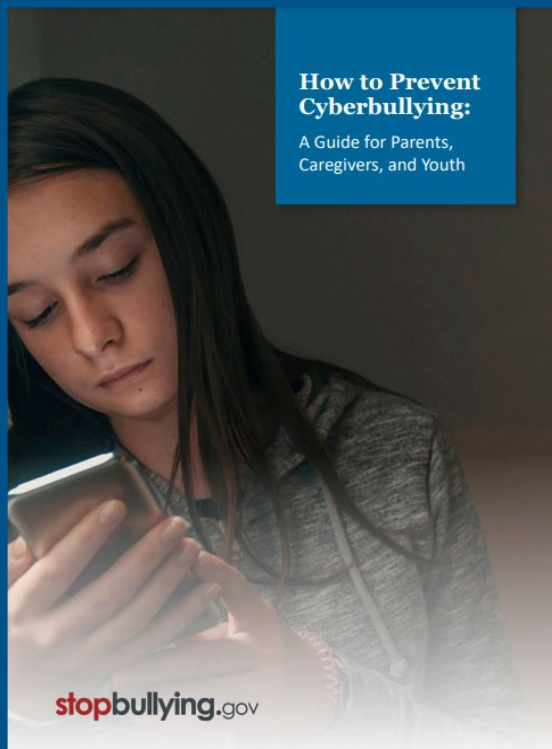
[www.cdc.gov](http://www.cdc.gov)



## Protecting Your Child from Electronic Aggression (CDC)

### How to Prevent Cyberbullying:

A Guide for Parents,  
Caregivers, and Youth



[stopbullying.gov](http://stopbullying.gov)

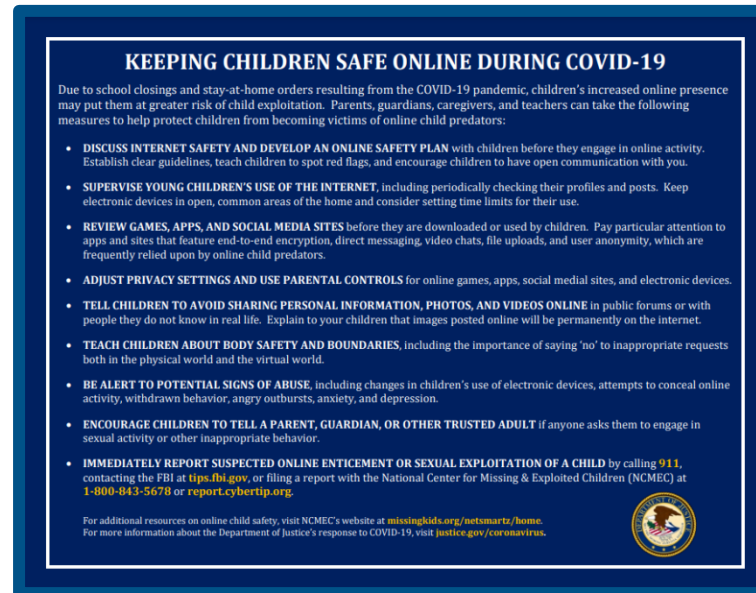
## How to Prevent Cyberbullying (Stopbullying.gov)



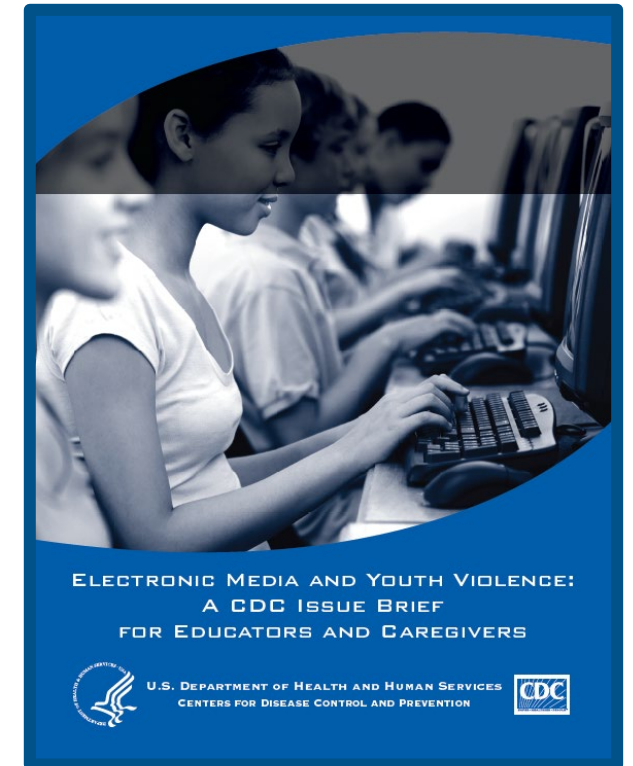
# Additional Resources



Bug Bytes  
(CISA)



Keeping Children Safe Online During COVID-19  
(DOJ)

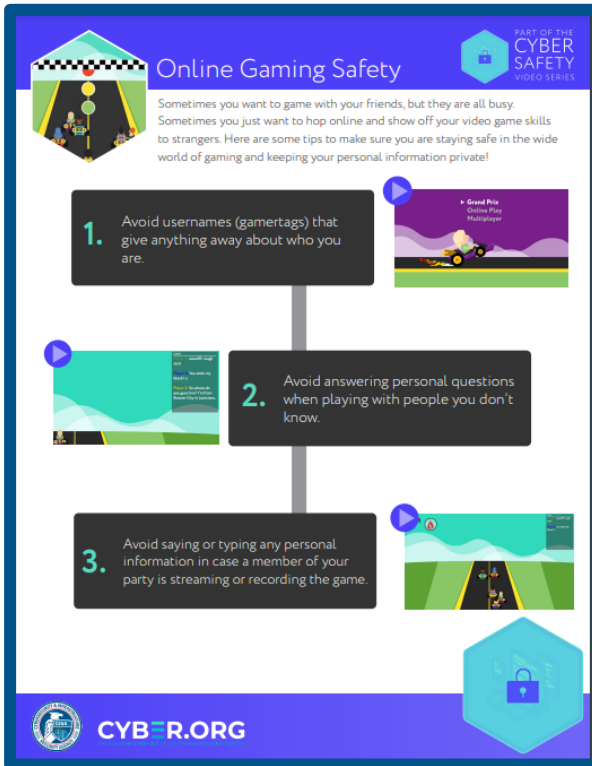


Electronic Media and Youth Violence  
(CDC)





# Additional Resources – Cyber Safety Series



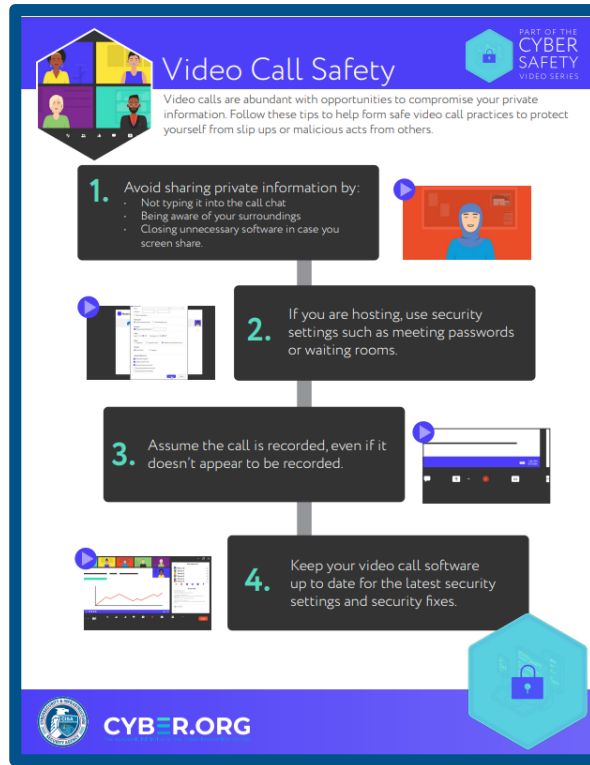
**Online Gaming Safety**

Sometimes you want to game with your friends, but they are all busy. Sometimes you just want to hop online and show off your video game skills to strangers. Here are some tips to make sure you are staying safe in the wide world of gaming and keeping your personal information private!

1. Avoid usernames (gamertags) that give anything away about who you are.
2. Avoid answering personal questions when playing with people you don't know.
3. Avoid saying or typing any personal information in case a member of your party is streaming or recording the game.

**CYBER.ORG**

Online Gaming Safety Tip Card  
(CISA and Cyber.org)



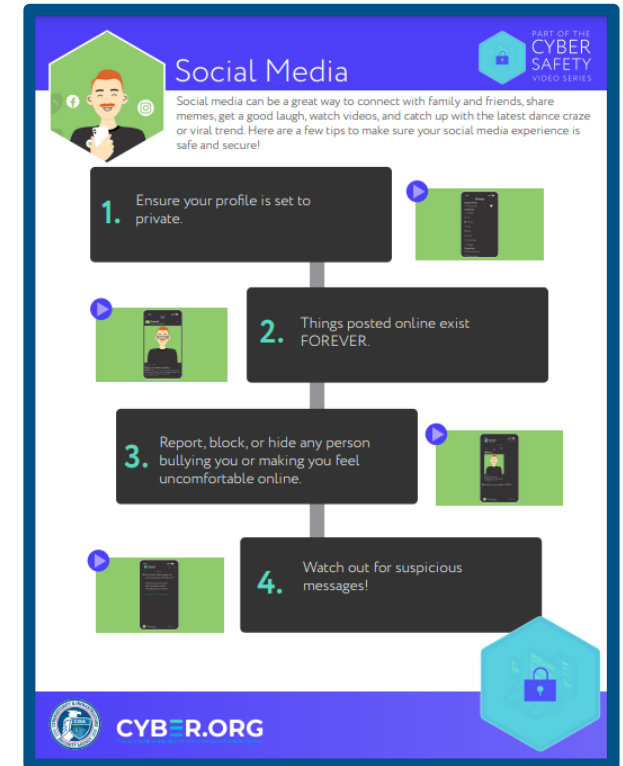
**Video Call Safety**

Video calls are abundant with opportunities to compromise your private information. Follow these tips to help form safe video call practices to protect yourself from slip ups or malicious acts from others.

1. Avoid sharing private information by:
  - Not typing it into the call chat.
  - Being aware of your surroundings.
  - Closing unnecessary software in case you screen share.
2. If you are hosting, use security settings such as meeting passwords or waiting rooms.
3. Assume the call is recorded, even if it doesn't appear to be recorded.
4. Keep your video call software up to date for the latest security settings and security fixes.

**CYBER.ORG**

Video Call Safety Tip Card  
(CISA and Cyber.org)



**Social Media**

Social media can be a great way to connect with family and friends, share memes, get a good laugh, watch videos, and catch up with the latest dance craze or viral trend. Here are a few tips to make sure your social media experience is safe and secure!

1. Ensure your profile is set to private.
2. Things posted online exist FOREVER.
3. Report, block, or hide any person bullying you or making you feel uncomfortable online.
4. Watch out for suspicious messages!

**CYBER.ORG**

Social Media Safety Tip Card  
(CISA and Cyber.org)

# CISA K-12 School Security Guide

The **CISA K-12 School Security Guide (3rd Edition)** provides a comprehensive doctrine and systems-based methodology to support schools in conducting vulnerability assessments and planning to implement layered physical security elements across K–12 districts and campuses. Available [here](#).

The guide is organized across three sections that aim to:

- Enhance understanding of a systems-based approach to layered physical security
- Explain the various elements of a comprehensive school security system
- Describe common challenges schools face in planning or making improvements



Accompanying Training Suite (Release: May 2022)	 Web-Based User Training
	 Train-the-Trainer Toolkit





# CISA K-12 Security Assessment Tool

The **CISA K-12 School Security Assessment Tool (SSAT)** is a web-based program that offers stakeholders a vulnerability analysis and provides recommendations for improving physical security based on provided specifications.

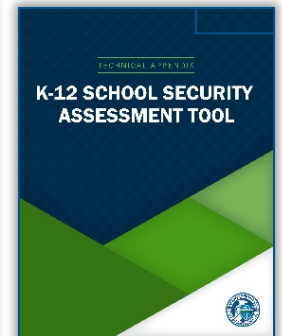
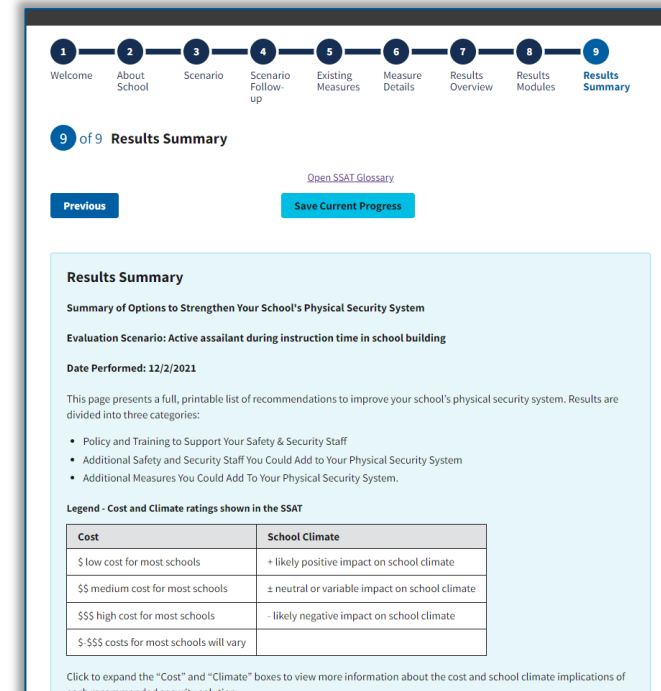
## HOW TO USE THE SSAT



The tool has launched with the K-12 Guide and:

- Is highly portable
- Is simple in language & design
- Serves all users, regardless of level of expertise
- Prioritizes results
- Recommends immediate actions

Now available at [CISA.gov/k-12-school-security-guide](https://CISA.gov/k-12-school-security-guide).



# Contact Information and Questions

Follow Us on Twitter for Upcoming Events and School Safety News! 

- [@SchoolSafetyGov](https://twitter.com/SchoolSafetyGov)
- [@HSI\\_HQ](https://twitter.com/HSI_HQ)
- [@NetSmartz](https://twitter.com/NetSmartz)

Click [here to sign up](#) for regular updates or scan QR code.

## Key Resource Links

- <https://SchoolSafety.gov>
- <https://www.ice.gov/partnerships-centers/cyber-crimes-center>
- <https://www.missingkids.org/netsmartz/resources>



Questions, feedback, or ideas?

Please contact [SchoolSafety@hq.dhs.gov](mailto:SchoolSafety@hq.dhs.gov)

SchoolSafety.gov

