Online Safety Guidance and Resources for K-12 Schools

Thursday, February 24, 2022
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
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)

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

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

What her gaming character looks like

What you think she looks like

What she really looks like
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

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 though Project iGuardian in 2021
• Developed in partnership with the National Center for Missing and Exploited Children’s NetSmartz
• https://www.ice.gov/topics/iGuardians
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.
Protecting the Homeland with Honor, Service, and Integrity

Q & A
Online Safety Resources

Susan Kennedy
Senior Program Manager, Outreach & Prevention
OUR MISSION

Find Missing Children
Reduce Child Sexual Exploitation
Prevent Future Victimization

Hope is why we’re here.
Internet Safety

Connect  Learn  Engage
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
## Prevention Education & Community Outreach Tools

<table>
<thead>
<tr>
<th>Free, interactive</th>
<th>Point-in-time delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age-appropriate</td>
<td>Training &amp; technical assistance</td>
</tr>
<tr>
<td>Data-informed</td>
<td>Spanish-language materials available</td>
</tr>
<tr>
<td>Customizable</td>
<td></td>
</tr>
</tbody>
</table>
• Netiquette
• Looking at inappropriate content
• Pop-ups/passwords
• Not trusting everyone you meet online

With Younger Children

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 – 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”
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?
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
Help Removing Sexually Explicit Content

Is Your Explicit Content Out There?

Search for Missing Children
AMBER Alerts
State Missing Persons Clearinghouses

CyberTipline
Exploitation Resources

24-Hour Hotline
Search Missing Persons
Make a CyberTipline Report
AMBER Alerts

Facebook Google YouTube Imgur Instagram Microsoft Tumblr Twitter Snapchat TikTok Kik
• 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
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

**Resilience Series**

**Bug Bytes**
(CISA)

**Keeping Children Safe Online During COVID-19**
(DOJ)

**Electronic Media and Youth Violence**
(CDC)
Online Gaming Safety Tip Card
(CISA and Cyber.org)

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

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

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.
Follow Us on Twitter for Upcoming Events and School Safety News! 🌐
• @SchoolSafetyGov
• @HSI_HQ
• @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