



Incorporating Sextortion Prevention, Response, and Recovery into School EOP Planning



U.S. Department of Education
Office of Safe and Healthy Students

Housekeeping

- To download a copy of the presentation slides and other pertinent handouts, use the Downloads Box on your screen. Select the name of the handout(s) you want and click the “Download File(s)” button.
- There is no dial-in for this webinar. Audio is available via the link provided. If you are experiencing difficulty hearing the audio stream, make sure your computer speaker volume is turned up.
- If you experience technical difficulties during the webinar, please contact the REMS TA Center at info@remstacenter.org or 1-855-781-REMS [7367]. You may also request technical assistance using the Q&A Tool. These questions are viewable to the webinar moderator only.
- If you would like to submit questions during the question and answer portion of this Webinar and are not able to do so via the box provided via Adobe Connect, please email your questions to info@remstacenter.org.

Questions & Answers

Please pose any questions using the Q&A Tool on the lower right side of your computer screen.

Agenda

Webinar Introduction and Purpose

Overview of the Issue

A Look at Federal, State, and Local Agency Collaboration to Support the Issue

Relation to School Emergency Management and EOP Development

Question and Answer Session

INTRODUCTION AND PURPOSE

Students can be both
sextortion victims
AND perpetrators

Schools and school
districts can be liable
for the
consequences

Education agencies
need to develop
measures to prevent
and protect students
from sextortion

What is “sextortion”?

A threat to distribute private and sensitive material if a victim does not provide images of a sexual nature, sexual favors, or money

<https://www.fbi.gov/video-repository/newss-what-is-sextortion/view>

Where does sextortion happen?

Where sextortion happens

54%

Social networks

41%

Messaging & Photo apps

9%

Dating apps

4%

Gaming platforms



Source: <http://money.cnn.com/2016/06/23/technology/sextortion-thorn-study/>

Who are the perpetrators?

Often disguise their identity and/or use the identity of others to develop rapport and trust between themselves and victims.

May be adults or other youth.

May or may not know the person targeted.

Sextortion PSA from U.S. Department of Justice and NCMEC

Online Enticement - A Look at a New Epide...

I'd love to see you.

You are so hot!

**ONLINE ENTICEMENT
SEXTORTION PSA**

How are schools involved?

Recent stories in the news show us that:

- Perpetrators often use a victim's fear that their personal or sensitive images will be exposed to other students and/or members of the school community as a means to commit sextortion.
- Educational agencies can face consequences for failing to respond to reports of sextortion affecting students.
- Educational agencies can play a vital role in prevention, response, and recovery.

OVERVIEW OF THE ISSUE

Kevin Gutfleish

Federal Bureau of Investigation

Criminal Investigative Division

Violent Crimes Against Children Section

Stacy Jeleniewski, PhD

National Center for Missing and Exploited Children

Exploited Children Division

Results from the National Child Exploitation Threat Assessment

The exponential rise of camera-enabled computer & mobile devices has yielded an exponential rise in sexual exploitation of children via these devices.

60% of survey respondents to the Dept. of Justice “National Strategy for Child Exploitation Prevention and Interdiction” indicated sextortion was an increasing threat.

Sextortion victims are engaging in cutting and other forms of self-harm at an alarming rate; and commonly exhibit depression and declining grades.

Results from the National Child Exploitation Threat Assessment

In 23% of the cases analyzed, FBI analysis determined a sextortion victim committed or attempted suicide.

There are documented cases of online sextortion victims being as young as 9 yrs old.

Sextortion victims have also been forced to sexually exploit other children, including younger siblings and friends.

Results from the National Child Exploitation Threat Assessment

Sextortion perpetrators have significantly more victims than perpetrators of all other crimes against children

In addition to the countless sextortion victims who are forced to share explicit material, there are significantly more kids willingly sharing explicit content online without being forced to do so.

- Such victims are being coerced and sexually exploited without their knowledge; and are also prime targets to be sextorted.

NCMEC CyberTipline

The CyberTipline functions as a clearinghouse:

- Reports taken from the public and Internet companies
- Value added to reports
- Reports sent out to Law Enforcement
- Internet companies notified, if necessary
- Follow-up with Law Enforcement and Internet Companies

What did NCMC review?

Examination of 801 CyberTipline sextortion reports

- Oct. 2013 through June 2015

Offenders:

- Primarily male
- Age was often too difficult to determine
- Primarily strangers

Children:

- Primarily female
- Ages ranged from 8-17 years old with an average age of 15 years old.

Reporters:

- Primarily self-, parent-, or Internet company reports
 - Female children had a greater variety of reporters

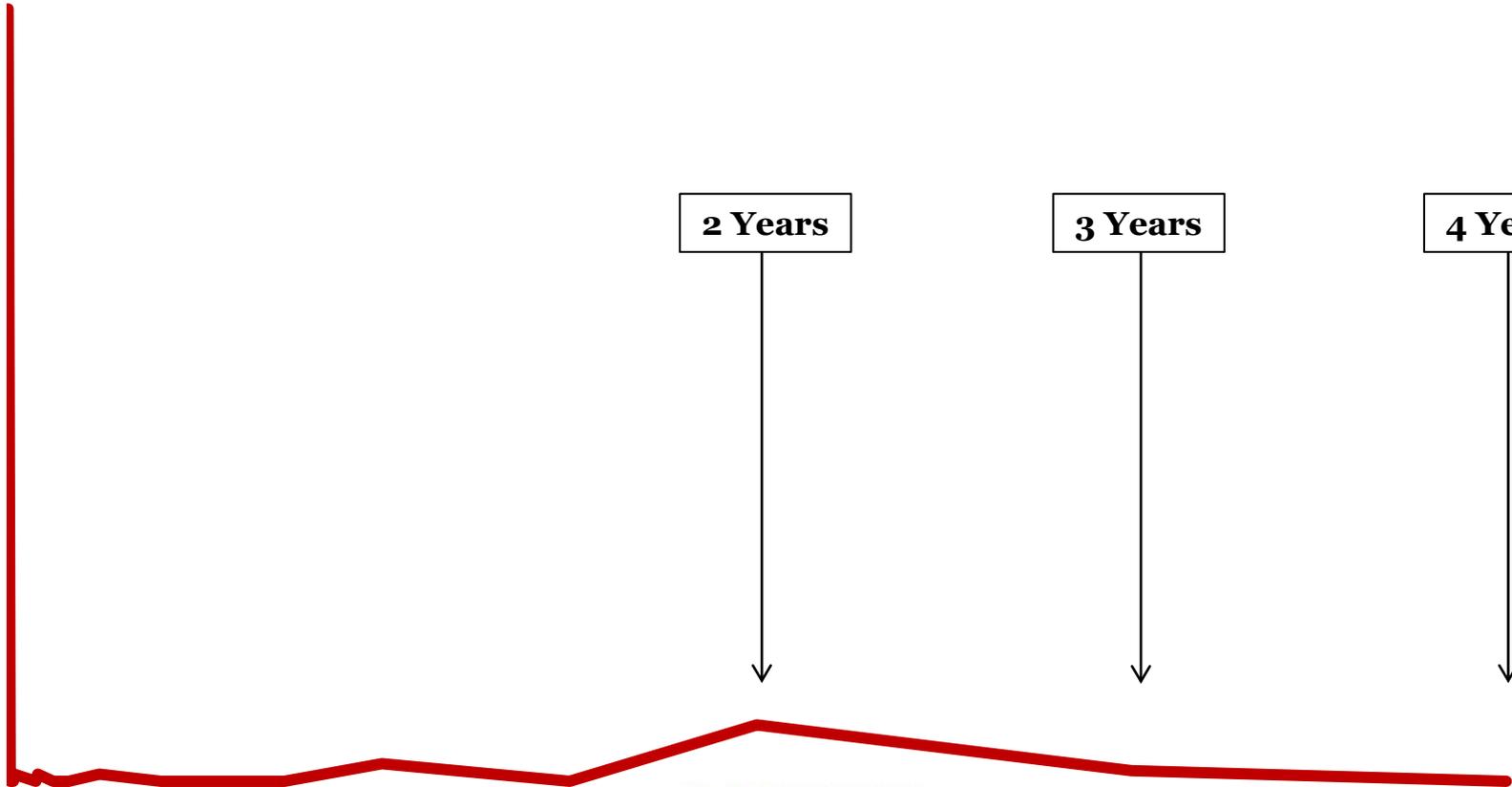
How quickly does sextortion begin?

Immediately

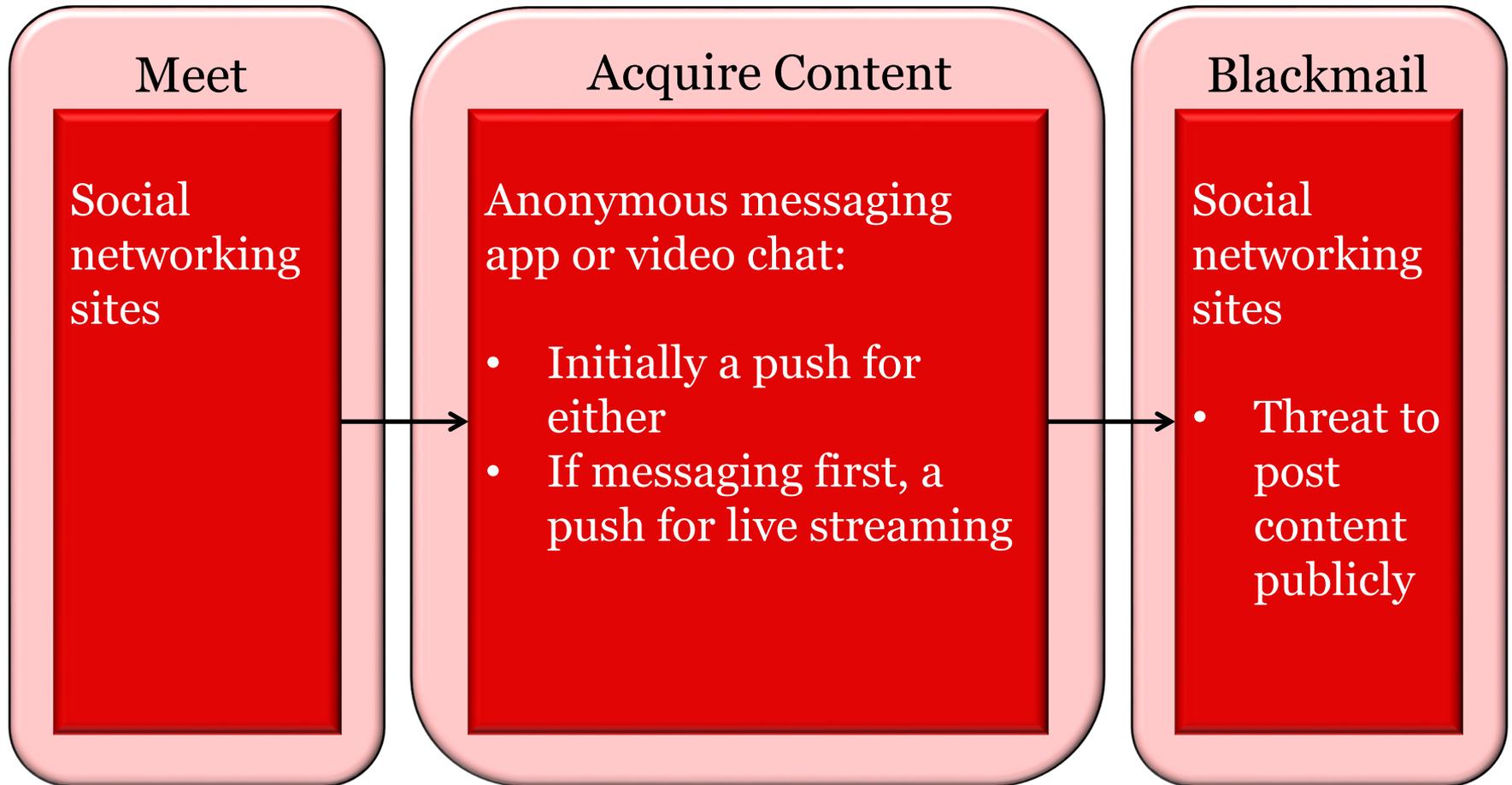
2 Years

3 Years

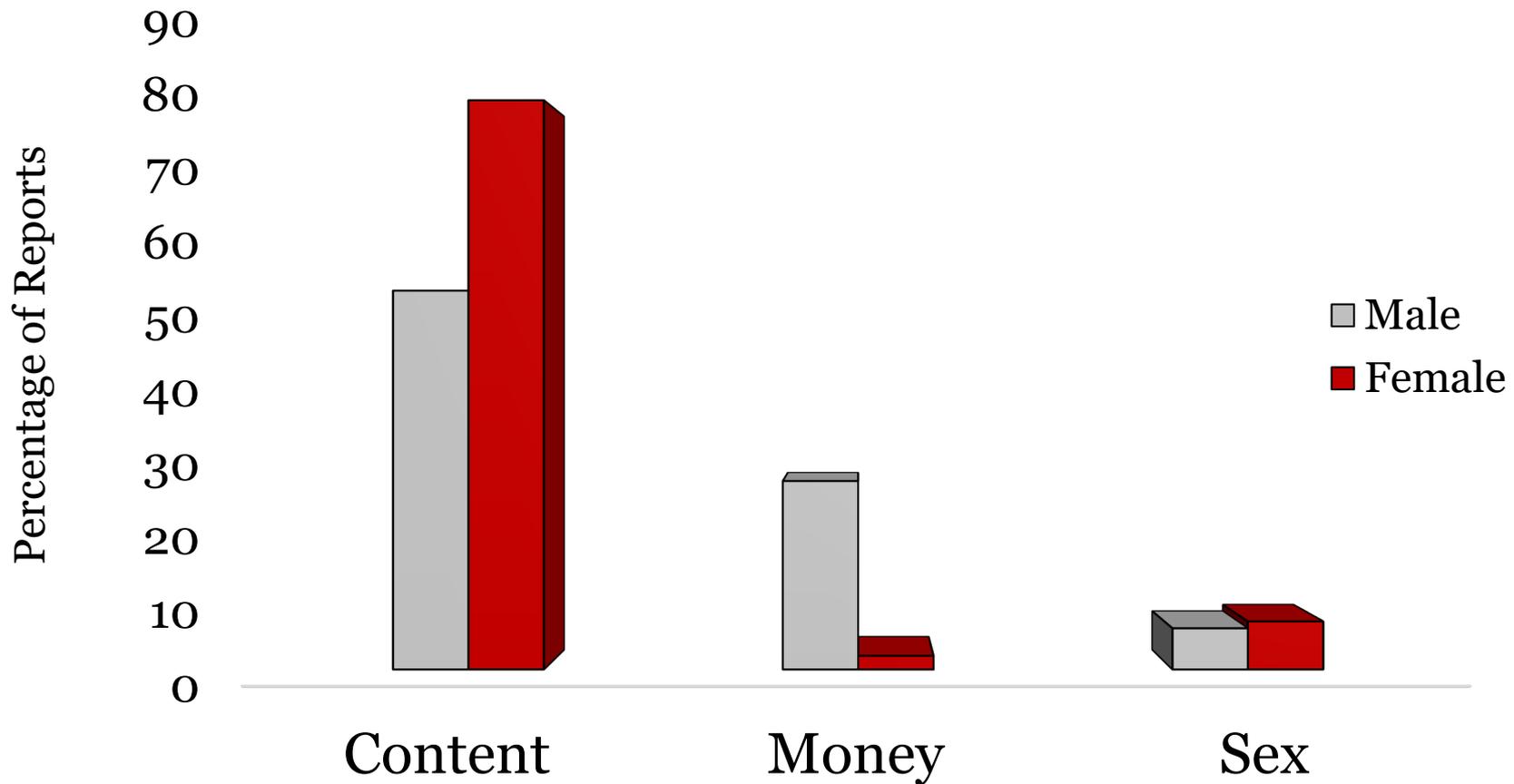
4 Years



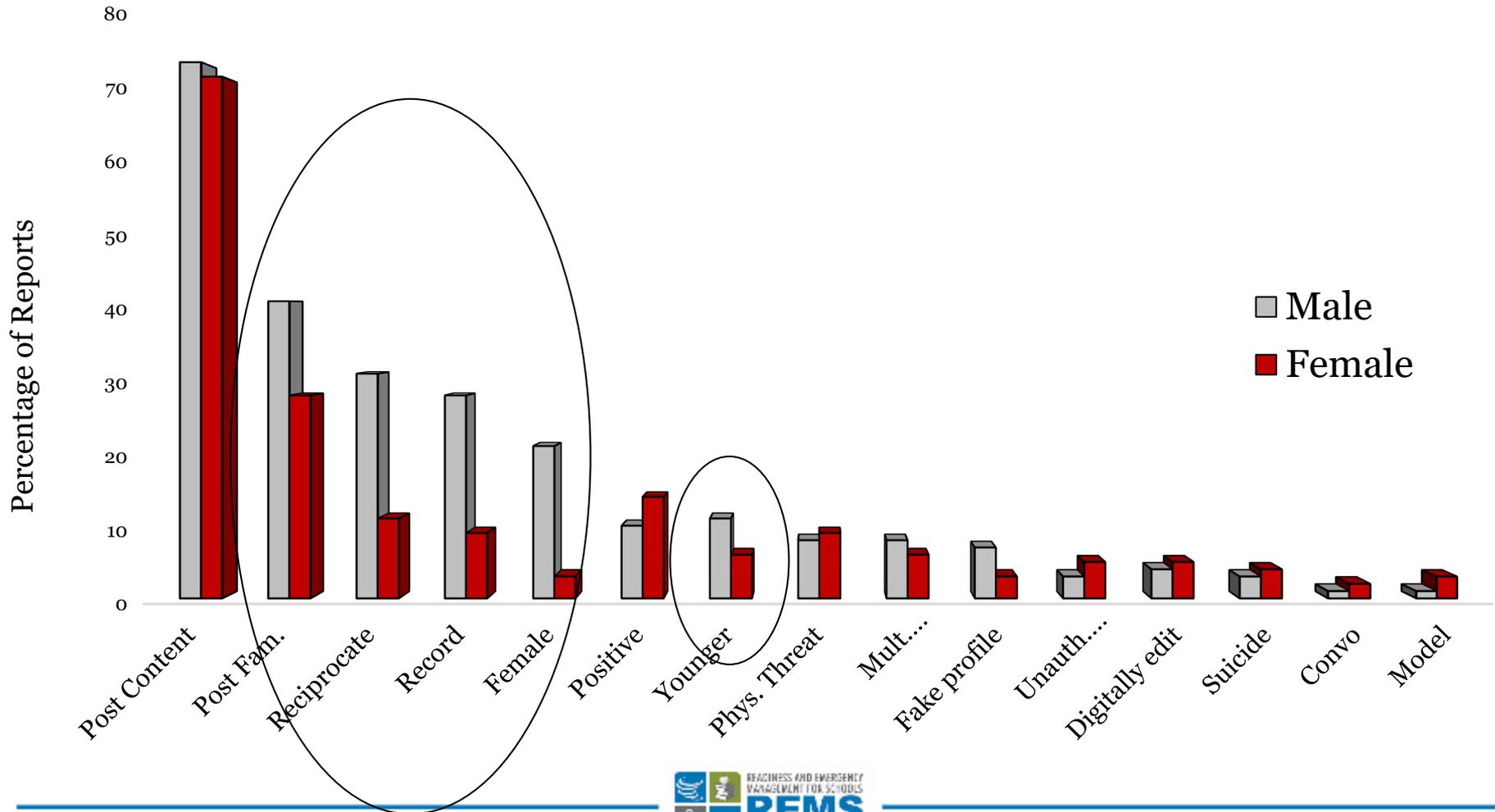
What is the pattern on multiple platforms?



Offenders' apparent motives for sextortion



Offenders' methods of manipulation by child gender



Negative Outcomes of Sextortion

A variety of negative outcomes were reported:

- Hopelessness, fear, anxiety, self-harm, suicidal ideation and even suicide attempts

Certain manipulation tactics made negative outcomes more likely:

- Threats to assault or rape the child (or family)
- Threats to post/send sexually explicit content of the child to their family/friends.
- Developing a positive rapport was associated with child suicide threats/attempts.

Prevention, Intervention and Collaboration

Informs in-house prevention/intervention efforts

Increases knowledge and awareness about this issue with the public

- Fact sheet
- PSA

Has allowed for collaboration with other NGO's and federal agencies

- Thorn
- FBI

Prevention, Intervention and Collaboration

THE GOOD NEWS IS...

Sextortion may be the fastest-growing form of child sexual exploitation...BUT it is also the most preventable!

A LOOK AT FEDERAL, STATE, AND LOCAL AGENCY COLLABORATION TO SUPPORT THE ISSUE

Jackie O'Reilly, Program Manager

Youth Development and Safety Division
Office of Juvenile Justice and Delinquency
Prevention

U.S. Department of Justice

Matthew Joy, Director

Wisconsin Department of Justice
Wisconsin Internet Crimes Against Children Task
Force

Internet Crimes Against Children (ICAC) Task Force Program

The ICAC program is a national network of 61 coordinated task forces representing over 3,500 federal, state, and local law enforcement and prosecutorial agencies.

These agencies are engaged in both proactive and reactive investigations, forensic investigations, and criminal prosecutions.

By helping state and local agencies to develop effective, sustainable responses to online child victimization – including responses to the online sharing of child sexual abuse images, OJJDP has increased the capacity of thousands of communities across the country to combat Internet crimes against children.

Why was this program developed?

Response to the increasing number of children and teenagers using the Internet

The proliferation of child sexual abuse images available electronically

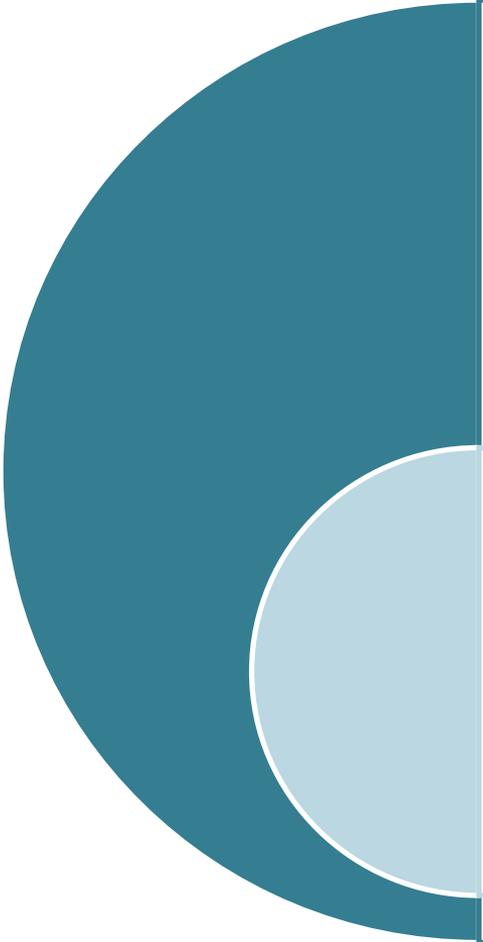
Heightened online activity by predators seeking unsupervised contact with potential underage victims

ICAC Task Force Program (continued)

OJJDP created the ICAC Task Force Program under the authority of the fiscal year (FY) 1998 Justice Appropriations Act, Public Law 105–119.

The program works under the Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act ("the PROTECT Act") of 2008, (P.L. 110-401, codified at 42 USC 17601, et seq.).

ICAC Task Force Program (continued)



Helps state and local law enforcement agencies develop an effective response to technology-facilitated child sexual exploitation and Internet crimes against children

This help encompasses forensic and investigative components, training and technical assistance, victim services, and community education.

ICAC Task Force Program (continued)

Since inception in 1998, more than 500,000 law enforcement officers, prosecutors, and other professionals have been trained on techniques to investigate and prosecute ICAC related cases.

In 2015, ICAC task force programs conducted more than 54,000 investigations and 61,000 forensic exams and trained over 34,000 law enforcement personnel, over 3,600 prosecutors, and more than 9,400 other professionals working in the ICAC field.

Since 1998, ICAC Task Forces have reviewed more than 580,000 complaints of alleged child sexual victimization resulting in the arrest of more than 60,000 individuals.

Current Trends & Themes from the Field

Evolving Levels of Sophistication and Brazenness

- “Known” Victims
- Children as Victimizers
- Hidden Apps | Shared Passwords
- Increased Demands

Victim Response

The “Aftermath” in and for Schools

Criminal Justice Systems: Responses

Examples from the Field

Central
Wisconsin

The Crush

Central
Wisconsin

The
Breakup

Southeast
Wisconsin

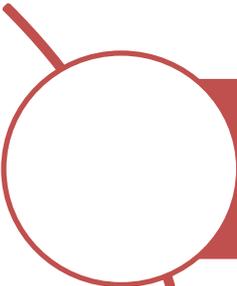
The “New”
Student

RELATION TO EOP DEVELOPMENT AND EMERGENCY MANAGEMENT PLANNING

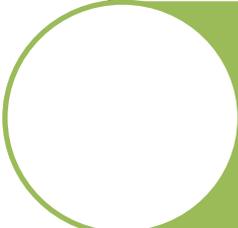
**Janelle Williams Hughes, Director of
Communications**

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

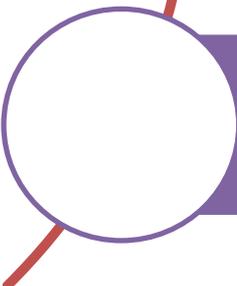
Why integrate sextortion into school EOPs?



All schools have or should have an emergency operations plan (EOP).



The goal of an EOP is to keep the whole school community safe before, during, and after a threat or hazard occurs.

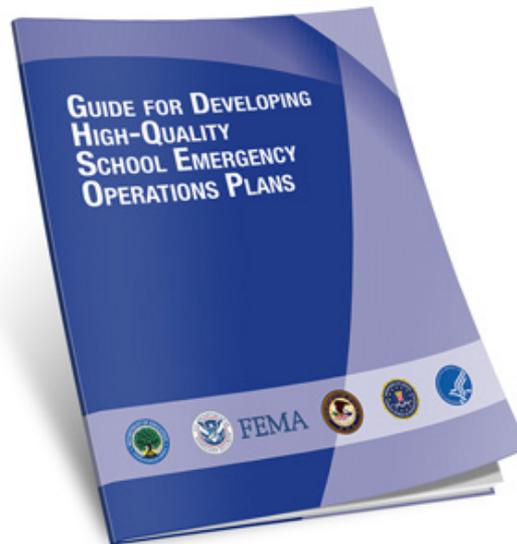


EOPs address more than natural disasters; they also address adversarial- and human-caused threats.

Federal Agency Partners



FEMA

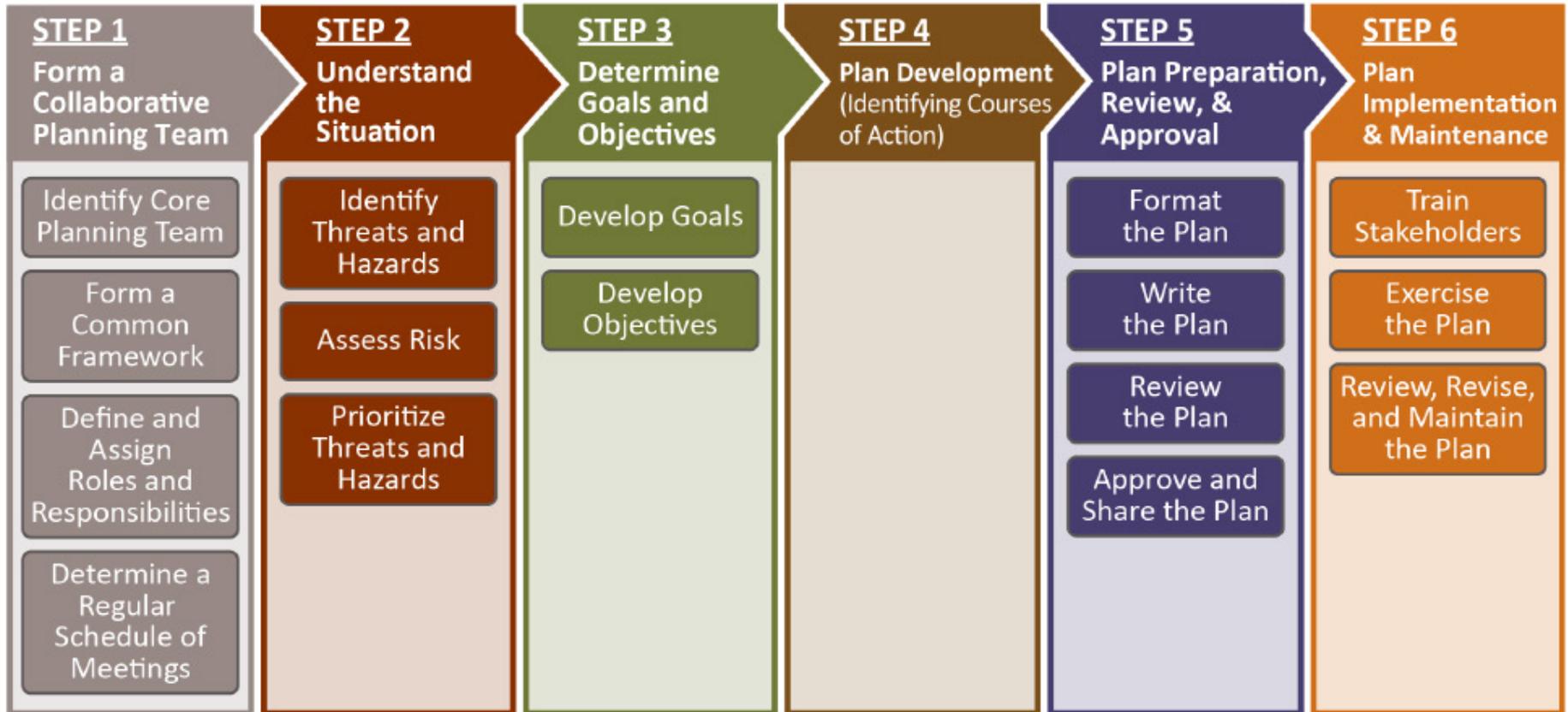


Five Preparedness Missions

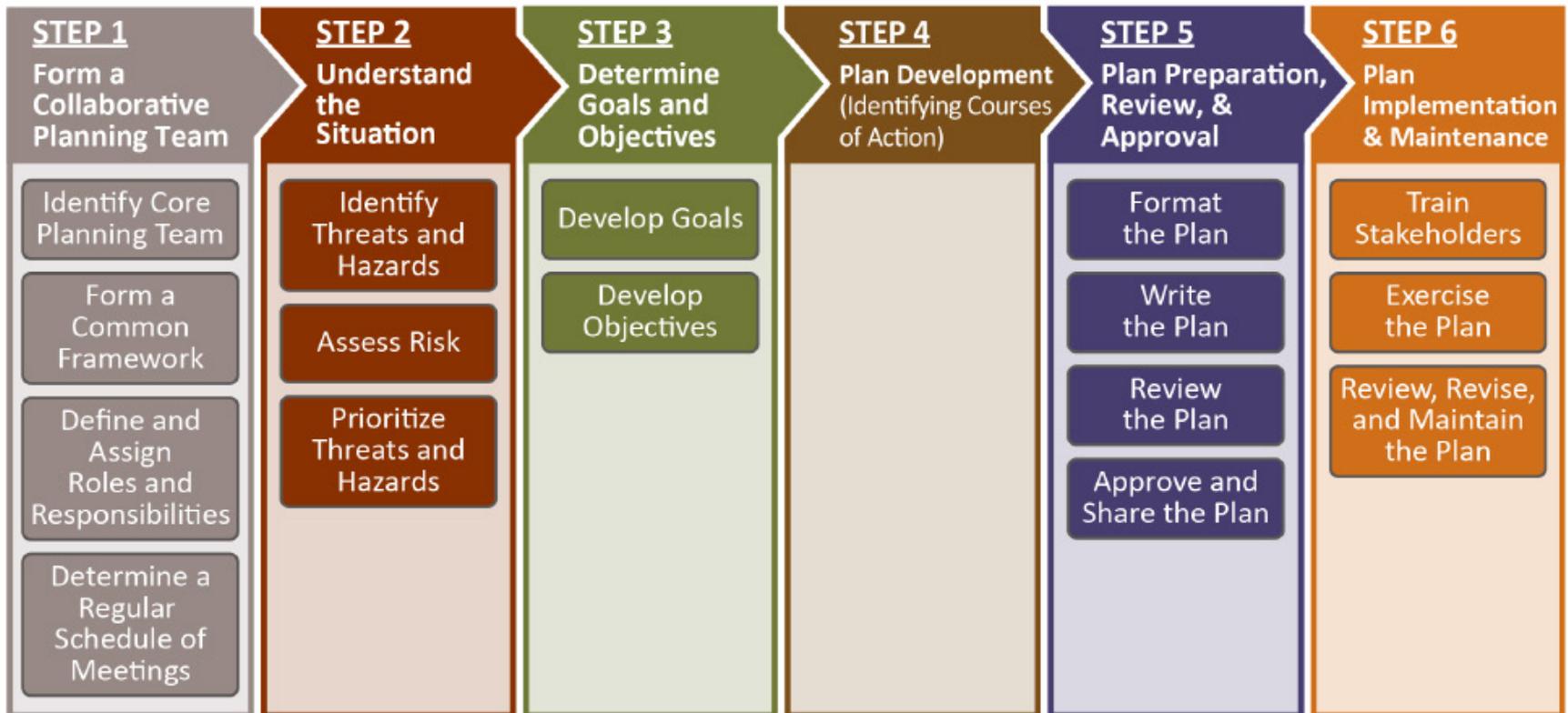


an incident or emergency

Steps in the Planning Process



Steps in the Planning Process



Sample Goals and Objectives to Address Sextortion

Sextortion Goal Example 1
(before): Prevent a student from becoming a sextortion victim or predator.

- Objective 1.1: Add a sextortion prevention training for all students and staff as a part of health education, cyber safety and security, and/or anti-bullying programs.

Sextortion Goal Example 2
(during): Using reporting and intervention services in collaboration with law enforcement and mental health partners.

- Objective 2.1: Require reporting all incidents of sextortion to the proper authorities.

Sextortion Goal Example 3 (after):
Provide restoration services to students to reintegrate them back into the learning environment.

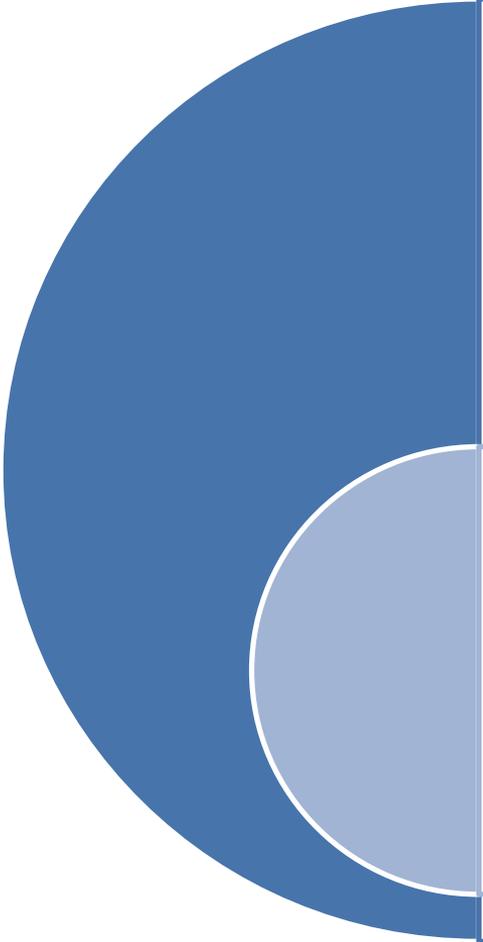
- Objective 3.1: Provide continued school counseling services to survivors of sextortion.

Action Steps to Address the Issue

There are various methods schools and school districts can use to address this issue. A comprehensive sextortion program, addressing protection, prevention, response, and recovery, may include courses of action for the following populations:

- School Emergency Managers
- School Instructional and Curriculum Development Staff
- School Mental Health Staff
- Teachers
- Students
- Community Partners
- Parents/Guardians

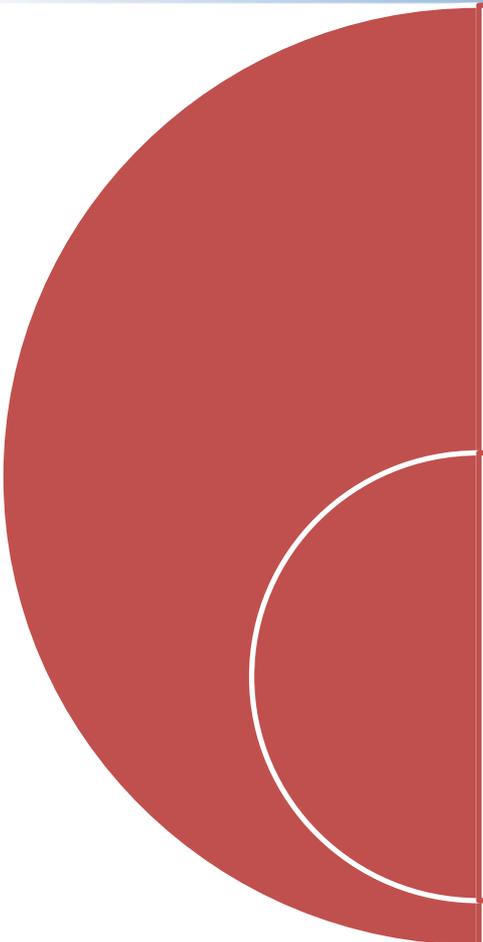
Action Steps for School Emergency Managers



Add sextortion to the list of adversarial and human-caused threats within school EOPs

Develop goals, objectives and courses of action for faculty, staff, and community partners, including law enforcement.

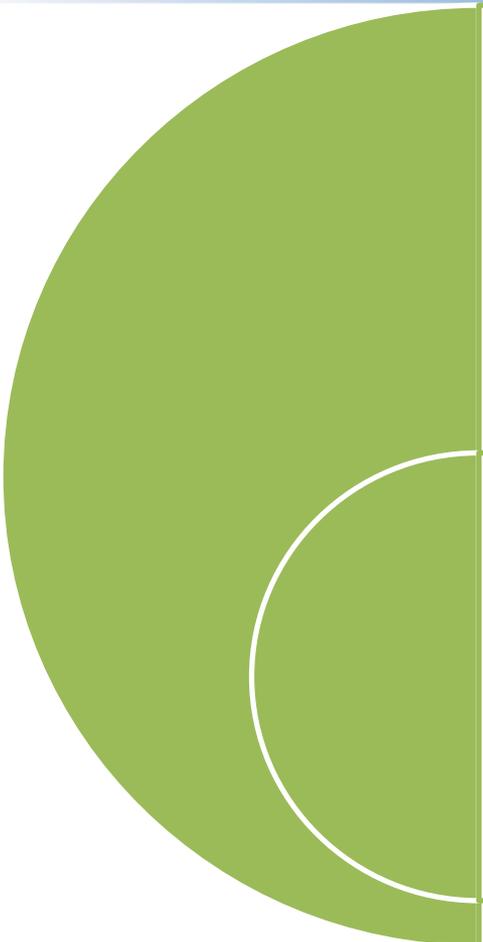
Action Steps for School Curriculum Development Staff



Include instructional materials on sextortion as a part of health education, cyber security, technology, computer literacy, and/or anti-bullying programs and/or curriculums

Conduct train-the-trainer sessions so that information can be easily communicated to new teachers and staff

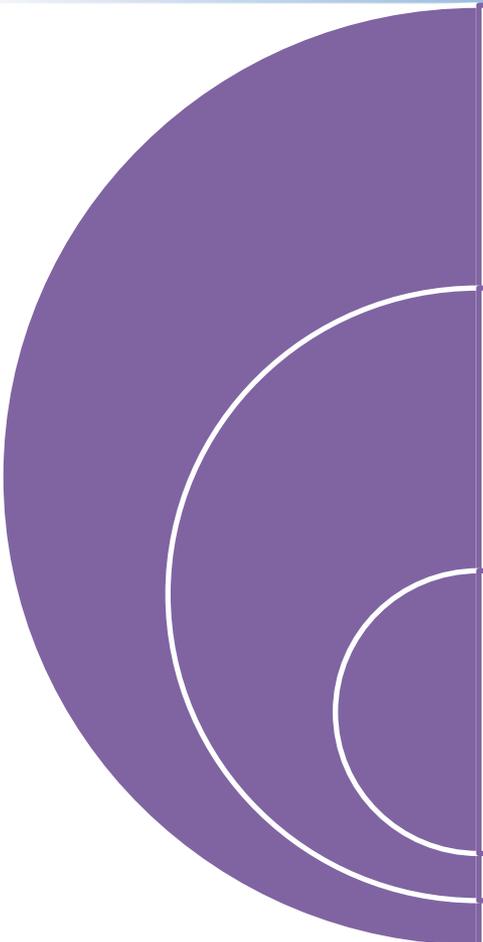
Action Steps for School Mental Health Staff



Train school counselors and mental health practitioners on risk factors and signs of students who are or may become victims or perpetrators of sextortion.

Train them on how to implement counseling services to support sextortion survivors, perpetrators, and families.

Action Steps for Teachers



Create checklists for teachers on what to do when they suspect a student has become a victim of or is perpetrating the crime of sextortion.

Create flyers that teachers can use to promote daily cyber safety practices among students

Engage students in developing flyers

Action Steps for Students

Create a peer-to-peer network of student leaders who encourage students to report incidents of sextortion, suspected perpetrators, and to not participate in the photo-sharing aspect often associated with the crime.

Share information about tip lines available through Federal and local agencies that students can use to report sextortion

Action Steps for Community Partners

Develop MOUs and Memorandums of Agreement with community partners that outline how you will work together to report, respond to, and help students and school communities recover from cases of sextortion

Conduct a Capacity Assessment to determine gaps in prevention planning and how you can work with partners to close those gaps

What else can schools do?

Plan to encounter students who are victims (or know a victim) because sextortion is happening nationwide right now and is increasing.

- Victims are more likely to report victimization to friends, students, parents, or teachers vs. the police or the FBI.

Address sextortion as part of school Internet safety programs and actively encourage victims of any abuse or exploitation to come forward.

- Students and victims feel more comfortable sharing when they know someone cares.

What else can schools do?

Create a safe and understanding environment to intake reports of what could be embarrassing and/or inappropriate behavior by a student.

Reassure victims they will not be prosecuted for sending explicit images (i.e. producing child pornography)...if they were forced to send them.

Reassure victims that coming forward will help countless other past, current, and future victims.

What else can schools do?

Advise victims that their exploitation is not likely to stop without intervention from law enforcement (even if the perpetrator promises otherwise).

Advise victims not to delete anything they sent, received, and/or posted, since it could be evidence of a crime and needed by law enforcement.

Notify law enforcement immediately.

Discuss sextortion prevention tips with faculty and students.

Sextortion Prevention Tips

Anything done online could be available/shared/seen by others.

Any video chat session can be recorded without one's knowledge.

Perpetrators can easily misrepresent themselves online to appear as another student or as an adult seeking to befriend a child.

Perpetrators can show a recorded video of a child and make it appear as though it is a live video feed.

Set app and social networking site privacy settings to the strictest level possible.

Sextortion Prevention Tips

Anyone who asks a child to engage in any sexually explicit activity should be reported immediately to a parent, guardian, or law enforcement.

- The only guarantee to make a perpetrator stop is for them to be in jail.

Sextortion Prevention Tips

Kids are much more likely to become a victim of sextortion if they:

- Do anything online they feel is inappropriate or could be used against them
- Do anything online they do not want shared with their online social network
- Willingly share explicit photos with anyone online or via text message
- Engage in “sexting” - even with a boy/girl friend or trusted individual
- Communicate online or via text with anyone they do not know personally
- Befriend strangers on social media, gaming, or other forums/apps/sites
- Share/post content with strangers (even if it isn’t explicit/sexual)
- Share personal details/identifiers with strangers
- Are vulnerable to hacking and/or social engineering

Sextortion Prevention Tips

To help prevent sextortion perpetrated by hackers:

- Cover webcams when not in use to avoid surreptitious recording.
- Use updated anti-virus software at all times on all mobile and Internet-connected devices.
- Don't open attachments from anyone you don't personally know.

Where to Get More Information

Access the **Resource List** we created to supplement this Webinar. It features a list of sites, reports, and agencies that can support your efforts to develop sextortion prevention, response, and recovery.

Access the **Sextortion Prevention Tips** flyer, which features additional tips that schools may find useful in terms of every day emergency management, cyber safety training, and school safety.

Read the **Incorporating Sextortion into School Emergency Operations Plans Fact Sheet**, which provides background information on sextortion, a look at the issue today, the relation to emergency management planning, and methods to address it.

QUESTION AND ANSWER SESSION



As a reminder, please pose any questions by typing them into the Q&A Tool on your computer screen.

Further Information



Phone: (855) 781-7367 (REMS)
Email: info@remstacenter.org

<http://rem.s.ed.gov>

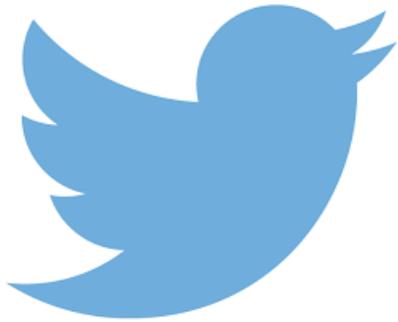
[Get the Guide](#)

[Join our Community of Practice!](#)

[Access Virtual Trainings](#)

[Request an On-site Training](#)

Twitter Chat



@REMSTACenter

#SextortioninSchools