What is Sextortion?

Sextortion is a criminal act that occurs when someone demands something of value, typically images of a sexual nature, sexual favors, or money, from a person by either:

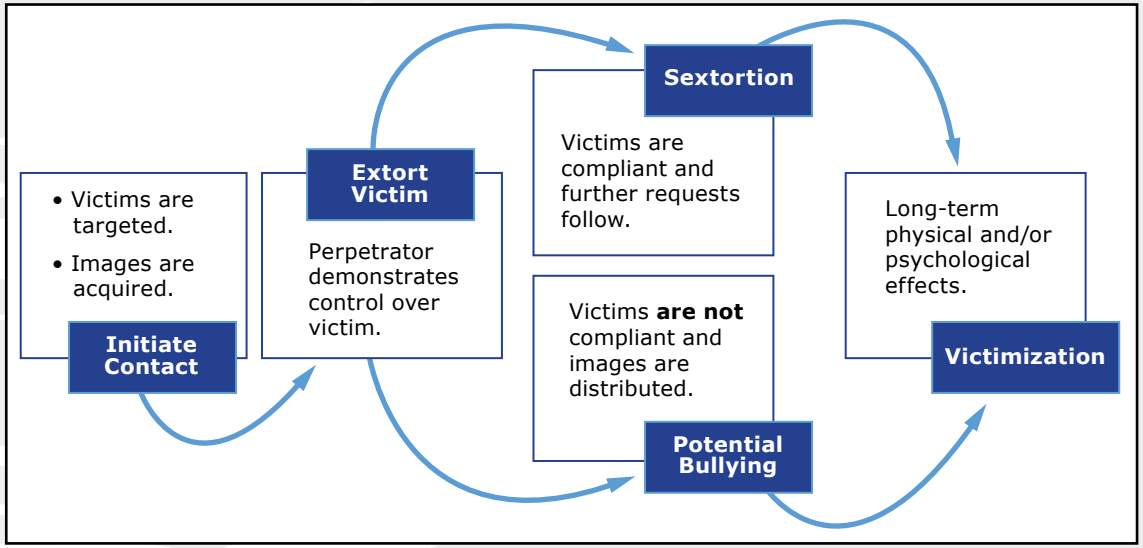
- Threatening to release or distribute material the victim seeks to keep private. This material often includes sexually explicit images, videos, e-mail, and text messages
- Threatening to financially harm friends or relatives of the victim by using information obtained from the victim's computer unless they comply with demands
- Withholding something the victim needs or wants unless they comply with demands. This is usually perpetrated by someone in a position of power or authority, such as a government official, educator, or employer

How Does Sextortion Happen?

Sextortion can be facilitated in many ways by those seeking to exploit vulnerable individuals sexually or for financial gain. They typically begin by obtaining sensitive material pertaining to their victims. Some of the methods include:

- Hacking or use of malware to assume control of a victim's computer, gaining access to the victim's files, and/or control of the computer's webcam and microphone
- Theft of personal electronic devices that contain sensitive material
- Social engineering -- leading the victim to believe the perpetrator can be trusted as the perpetrator represents himself/herself as a business (i.e. modeling agency), friend, or even the victim's boyfriend or girlfriend. This results in the victim releasing sensitive material to the perpetrator
- Identity theft

These tactics are typically conducted over the Internet or cellular networks using social networking sites (SNS), instant messaging, and e-mail. The diagram below illustrates a typical sextortion process:



How is Sextortion Related to "Sexting" and Bullying?

Sexting is the sending of sexually explicit images from one person to another using mobile devices. Sexting is one way images come into the possession of a perpetrator who could use them to facilitate the sextortion. When sexually explicit images of a student are distributed to their peers, those images often become the basis of intense bullying in a school environment.

Who is at Risk and What is the Impact?

Sextortion affects children across all demographics. Victims of sextortion withdraw from family members and can experience anxiety; psychological, physical and emotional trauma; bullying; increased risk for suicide; and increased dropout rates.

Examples of Sextortion Cases:

- ***In November, 2014***, Lucas Michael Chansler, 30, of Jacksonville, Florida, was sentenced to 105 years in prison for producing child pornography. During a four-year period, Chansler is believed to have sexually extorted approximately 350 victims in 26 states, three Canadian provinces, and the United Kingdom.
- ***In March, 2014***, Jared James Abrahams, a computer science student, was sentenced to serve 18 months in federal prison after pleading guilty to three counts of extortion and one count of unauthorized access of a computer. Abrahams targeted dozens of victims around the globe, including Miss Teen USA Cassidy Wolf. Abrahams used malicious software to disguise his identity in order to capture nude photos or videos of female victims through remote operation of their webcams without their consent.
- ***Between 2005 and 2009***, Ivory Dickerson and Patrick Connolly victimized more than 3,800 children through sextortion. Using malware, Dickerson and Connolly were able to assume control of the victims' computers and then demanded the victims send sexually explicit images of themselves. Dickerson was sentenced to 110 years in prison while Connolly was sentenced to 30 years in prison.

How Can I Protect Against Sextortion?

For Parents:

Supervise children's computer or mobile device usage. Devices like smartphones are more difficult to manage due to their mobility and technical capabilities. As teenagers' brains are not yet fully developed, they often struggle with anticipating consequences or impulse control. It's important to discuss with your children appropriate uses for

devices when they are given access to them. This includes communicating with others online and sending photos. Parents may want to maintain their child's online account access information with the child's understanding that the parent can log in at any time.

Communicate with your children.

Have age-appropriate discussions with your child about the dangers associated with communicating with unknown people online, sending photos, or engaging in other risky behavior online. In an effort to protect children from online predators, it's important to educate them about sextortion and the motivations of those who extort children. Let your children know they can come to you without fear of reprisal, and that you have a genuine interest in their safety and online activities. Those exploited through these crimes are victims, no matter what they did or how they responded to the threat.

Layer security.

Employ basic technology security measures. Use strong passwords and update software regularly. Never open attachments to e-mails unless you are certain of the sender. Use a firewall, anti-malware software, and consider use of encryption for your hard drive. Keep in mind that some malware attacks are targeted, meaning criminals may customize their tools so that more simplistic anti-malware programs do not detect them and victims are more apt to take the bait. Do not assume technology alone will protect you; you must also do your part to protect yourself.

For Children:

- Turn off your computer when you are not using it.
- Cover webcams with a removable sticker or tape when you are not using them.
- Don't open attachments when you're not confident of the sender.
- Never send compromising images of yourself to anyone, no matter who they are or who they say they are.
- If someone you know is being victimized through sextortion, report it to your parents and encourage the victim to talk to their parents and report it to the FBI.
- If you are receiving sextortion threats, don't be afraid to talk to your parents or to call the FBI.

How do I Report a Suspected Incidence of Sextortion?

Report sextortion to the FBI.

It is important to report all instances to law enforcement. While in some cases the person committing sextortion is also a teenager, it is more likely that the perpetrator is an adult masquerading as a teenager. Law enforcement can make that determination and take steps to help minimize further distribution of sensitive material. A parent's report may result in the rescue of dozens or even hundreds of other children.

To report suspected sextortion crimes or to get help from law enforcement, call your local FBI office or toll-free, at 1-800-CALL-FBI (225-5324).

Resources:

- The National Center for Missing and Exploited Children (www.missingkids.com)
- FBI Cyber Alerts for Parents and Kids: Be Prudent When Posting Images Online (http://www.fbi.gov/news/stories/2011/december/cyber_122211/cyber_122211)
- FBI Cyber Alerts for Parents and Kids: Be Aware of 'Sextortion' (http://www.fbi.gov/news/stories/2012/february/sextortion_021012)

July 2015

U.S. Department of Justice
Federal Bureau of Investigation

SEXTORTION OF CHILDREN IN THE UNITED STATES

A Fact Sheet for Parents and Children