Cyber Directorate
Department of the Army
Criminal Investigation Division

Cybercrime Prevention Flyer

CPF 00005-2023-CID461 **10 January 2023**

Sextortion

Sextortion, a combination of “sexual” and “extortion,” is the act of threatening to expose or distribute a sexual image or video unless a victim complies with certain demands. Sextortion scams are enacted across the internet and do not require the victim and criminal subject to be in the same location or have ever met in person. Sextortion victims can be children or adults. In the majority of offenses, the subject demands money in exchange for not releasing the sexual material.

Sextortion Prevalence

The widespread adoption and use of social networking sites and apps creates a fertile ground for criminals conducting sextortion offenses. Initial contact with multiple individuals can be established relatively quickly and “spamming” introduction messages to hundreds of potential victims is not uncommon. Criminals use the same personal profiles on multiple forums and use prerecorded videos while communicating with multiple victims simultaneously. Incidents that do not proceed to extortion are rarely reported, which allows the subject to continue their attempts unabated.

Relationships that begin on popular social networking sites give subjects access to the victim’s network of friends and family. The subject may use this access as part of their threat of embarrassment to distribute the images to a victim’s known contacts. The victim’s knowledge of who specifically will see the private images increases their likeliness to comply with the subject’s demands and reduces their willingness to report the sextortion.

Using the fear of exposure or the fear of criminal prosecution, the criminal demands the victim forward money through a money transfer agent (e.g., Cash App, Western Union, Moneygram, Zelle, etc.), that makes it difficult for the victim or law enforcement to trace. Criminals may order the payments be sent as cryptocurrency for this same reason. Technological developments have made cryptocurrency transactions easier to accomplish for criminals and victims and add another layer of detection difficulty.

Sextortion and Suicide

Sextortion victims have resorted to suicide when they believe they have no other options. In 2019, a 24-year-old Army veteran in South Carolina took his own life after meeting a criminal on Plenty of Fish, a social networking site, who extorted him for $1,200. In 2021, two minor victims in St. Lawrence County, New York committed suicide after being targeted through Facebook Messenger. In 2022, a teenager in California ended his life after he was extorted for $150.

Criminals prey on the fear of exposure and the anguish it will cause, especially for individuals who may feel they cannot ask for help or report the abuse when they are caught in this cycle. It’s important to talk about how sextortion occurs, how to protect oneself, and how to report it if you become a victim.

Report a crime to the Department of the Army Criminal Investigation Division

Cyber Directorate
27130 Telegraph Road
Quantico, Virginia 22134

Email

Cyber Directorate Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

Cybercrime Prevention Flyer

Protect Yourself

Anything posted online will essentially exist forever. Once something is out on the internet, it is nearly impossible to delete it completely or to take it back. Personal information, images, live video streams, and text messages cannot be recalled once sent. Think through the worst outcomes before sending something.

Overcoming the embarrassment and reporting sextortion is crucial to stopping it. Unreported extortion will result in continued harassment, even if the victim meets the initial demands.

Sextortion victims should:

- Not send money.
- Save all transaction records if money or cryptocurrency is sent.
- Report the offense to the banking system used to send money. This aids in flagging the receiving account as criminal.
- Contact law enforcement authorities as soon as possible and follow their instructions.
- Stop communicating with the criminal subject.
- Save all communications with the criminal subject, no matter the platform.
- Scan all computer devices for viruses and other malicious software.

Reporting Sextortion

Soldier victims of sextortion should contact their local CID office or report the incident via CID Crime Tips. Army civilians, dependents, contractors and Reservists and National Guard members not on active duty should report sextortion to their local law enforcement.

In addition to contacting CID or reporting to local law enforcement, victims should submit a report to the Internet Crime Center (IC3). IC3 provides a central reporting repository for law enforcement to connect similar victim reported incidents.

If a sextortion victim is showing signs of suicidal ideations or emotional distress, reach out to the National Suicide Hotline by phone at 988 or online.

Additional resources:

Sextortion Crimes on the Increase

FBI warns of explosion of 'sextortion' cases targeting boys, teens

These Social Media Scams Affect the Military

To receive future Cyber Directorate Cybercrime Prevention Flyers, send an email to: Subscribe CPF