United States Army
Criminal Investigation Command

Media contact:
571-305-4041

FOR IMMEDIATE RELEASE

Army CID Warns of Internet Sextortion Scams

QUANTICO, VA. (March 5, 2019) – As part of a continuing campaign to help prevent Soldiers and other members of the Army community from becoming victims of crime, Special Agents from the U.S. Army Criminal Investigation Command, commonly known as Army CID, are once again cautioning the Army community about ongoing Internet based "sextortion" scams.

Sexual extortion, or "sextortion," is a cybercrime perpetrated against unwitting victims who are often approached in casual conversation via social media platforms and then seduced into engaging in online sexual activities. After participating in the sexual request, which are most often recorded without the victim's knowledge or consent, the victim is then threatened by the criminals with public exposure and embarrassment if the victim does not pay money to the extortionist.

According to military officials, more than 450 known military members from all services have fallen victim to the scam and have been blackmailed for more than $560,000 dollars, and those numbers do not include the number of victims who have not come forward.

With the criminals threatening to send compromising video or photographs to the victim's commanders or families, victimized military members often pay out of fear that their careers will be jeopardized by the false claims. In another concerning version of the scam, the criminals will contact the victim and pose as police or parents of who they claim is an "underage victim" and threaten to ruin the service member's career or have them arrested if they do not pay the ransom.

Another method the criminals use to attempt to extort money is to claim that they are a lawyer working on behalf of the alleged victim. The scammer will request payments for things such as counseling for the alleged victim or to replace electronic devices that now contain alleged "child pornography." If these demands are not met, the person claiming to be the lawyer threatens to report the incident to law enforcement.

"Legitimate organizations will not contact you and ask for money in lieu of reporting you to law enforcement," said Special Agent Edward LaBarge, the head of Army CID's highly specialized Computer Crime Investigative Unit. "Typically law enforcement will not attempt to make contact with you over the phone. If you are contacted via telephone, always request validating information such as an agency email address and offer to meet in person at a law enforcement facility before proceeding with giving out your personal information."

Army CID officials stress that if an individual is being blackmailed and comes forward, they want to help that individual.

"It is important to also keep in mind that law enforcement, to include Army CID, will never agree not take legal action against you if you have agreed to pay [ransom] money to the alleged victim or to the alleged victim's family," LaBarge said.

-more-

“We encourage victims to contact us so we can help. If law enforcement gets involved early on, there are investigative steps that may help identify the perpetrators responsible for victimizing Army personnel.”

Additionally, CID officials warn that if you do not seek help, victims are often at risk for further exploitation. Once the blackmail begins, the criminals can continue to demand additional payments, more sexual images, sensitive military information, or access to U.S. Army systems and facilities, so early notification to law enforcement is very important according to CID Special Agents.

“To avoid falling prey to a sextortion scam, never send compromising photos or videos of yourself to anyone, whether you know them or think you know them,” said LaBarge. “You are also advised to turn off your electronic devices and physically block web cameras when you are not using them.”

For more information on how these scams unfold and how to identify sextortion red flags, see the Joint Service Sextortion brochure.

If you have been the victim of sextortion, adhere to the following:

- DO preserve whatever information you have from the scammer(s), such as social networking profile, email accounts used, where money was directed to be sent, etc.
- DO notify CCIU at usarmy.cciuintel@mail.mil to report being a victim if you are a service member or an Army civilian employee. If you are not associated with the military, report the crime to your local police department, DHS Homeland Security Investigations at Assistance.Victim@ice.dhs.gov, or the FBI’s Internet Crime Complaint Center at www.ic3.gov.

Victims can seek information on rights and assistance from:

- ArmyVictim/Witness Liaison Program - VWL will assist victim in contacting agencies or individuals responsible for providing necessary services and relief.
- Command Chaplains.
- Family Advocacy Center/Army Community Service.
- If victims are not eligible for military services, or where military services are not available, the VWL can provide liaison assistance in seeking any available nonmilitary services within the civilian community.

-30 –

For more information about computer security, other computer-related scams and to review previous cyber- crime alert notices and cyber-crime prevention flyers visit the Army CID CCIU website at https://www.cid.army.mil/cciu-advisories.html. To report a crime to CID, visit www.cid.army.mil.