United States Army
Criminal Investigation Command

Media contact:
571-305-4041

FOR IMMEDIATE RELEASE

CID: 'Sextortion' Scams continue to occur; don't give into scammer's demands

QUANTICO, VA. (April 26, 2018) – The U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU) continues to caution the Army community to be on the lookout for all types of "sextortion scams" where criminals will use any dishonest method to make contact with potential victims and then attempt to blackmail them.

"To avoid falling prey to a sextortionist never send compromising photos or videos of yourself to anyone, whether you know them or think you know them," said Special Agent Daniel Andrews, director of CCIU. "Turn off your electronic devices and physically block web cameras when you are not using them."

Officials describe "sextortion scams" as cyber sexual extortion where perpetrators conduct schemes that leverage online sexual acts for financial gain or other forms of blackmail.

In addition, when using a legitimate online dating site, victims are more apt to provide personal information and or participate in online "compromising acts;" however, CID officials are warning the Army community to be very cautious of their online communications activity and not share intimate, personal information with strangers or people you have never met in person.

"These criminals will try to get unsuspecting service members to engage in online sexual activities and then demand money or favors in exchange for not publicizing potentially embarrassing information or turning them over to law enforcement," said Andrews.

Once the Soldier sends a compromising photo or participates in a video chat, the perpetrator threatens to send those images to the Soldier's command, family, and friends unless "ransom money" is paid, according to CCIU officials. One recent scam is where the criminal will claim that the Soldier sent sexual images to a minor, who has now become the alleged victim, and threaten to report the Soldier to law enforcement unless a monetary fee is paid.

"If you meet a person on a legitimate online dating site there is very little chance that you are actually communicating with an underage person," Andrews said. "It is therefore very unlikely that you sent or received child pornography or provided your images/videos to a minor. If you met someone online who later claims to be underage you should immediately cease all communications with that person and notify Army CID."

- more -

add 2-2-2

Sextortion

“It is important to also keep in mind that law enforcement, to include Army CID, will never agree not take legal action if you agree to pay [ransom] money to the alleged victim or to the alleged victim's family,” he said. “If law enforcement gets involved early on, there are investigative steps that may help identify the perpetrators responsible for victimizing Army personnel.”

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

Andrews said legitimate organizations will not contact you and ask for money in lieu of reporting you to law enforcement and 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.

“Stop communication immediately with these individuals and do not send money because it will not stop the criminal from demanding more money from you,” CCIU officials said. “CCIU is aware of instances where scammers threatened to release videos unless a second or even a third payment is made.”

Unfortunately, these incidents continue to occur on the internet across the globe, and sextortion victims are encouraged to seek the assistance of law enforcement. Army CID agents say they can help if you find yourself in any of these types of predicaments.

“Victims are at risk of further exploitation, that can include demands for additional payments, more sexual images, sensitive military information, or access to U.S. Army systems and facilities, so early notification to law enforcement is important,” CID agents emphasized.

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.

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 http://www.cid.army.mil/cciu-advisories.html.

 # CID #

For more information on CID, visit www.cid.army.mil. To report a felony-level crime, provide information concerning a crime, or if you are the victim of a crime, contact your local CID Office, the Military Police, call 1-844-ARMY-CID (844-276-9243) or email CID at Army.CID.Crime.Tips@mail.mil.