United States Army
Criminal Investigation Command

Media contact:
571-305-4041

FOR IMMEDIATE RELEASE

Army CID Warns of ‘Sextortion’ Scams

QUANTICO, VA. (Feb. 1, 2017) – The U.S. Army Criminal Investigation Command’s Computer Crime Investigative Unit (CCIU) cautions Soldiers to be on the lookout for “Sextortion scams” where criminals will try to engage in online sexual activities with unsuspecting service members, and then demand money or favors in exchange for not publicizing potentially embarrassing information.

Officials describe “sextortion scams” as cyber sexual extortion in which perpetrators conduct schemes that leverage those sexual acts for financial gain or other forms of blackmail.

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 “hush money” is paid, according to CID special agents. Officials caution that Soldiers may be prime victims because they want to protect their career and out of embarrassment, they may reluctantly give in to the financial or other demands of the extortionist. CCIU agents added that this particular scam is sometimes effective because once the perpetrator gets the unsuspected Soldier to perform some sort of virtual sexual act with an “attractive person” on the Internet, while they are secretly recorded, the true nightmare begins because they are now more likely to be blackmailed for those compromising images.

-more-

“Be cautious of your online communications and do not share intimate, personal information with strangers or people you have never met in person,” said Special Agent Daniel Andrews, director of CCIU.

Unfortunately, these incidents continue to occur across the globe, and sextortion victims are encouraged to seek the assistance of law enforcement.

“Victims are at risk of further exploitation, which 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,” Andrews said.

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

- DO NOT send money to the scammer(s). CCIU is aware of instances where scammers threatened to release videos unless a second or even third payment is made.
- DO NOT continue to correspond with the scammer(s).
- 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 or 571-305-4478 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.

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.

#USACID#

For more information on CID or to report a felony-level crime or provide information concerning a crime, contact your local CID Office or the Military Police or visit www.cid.army.mil.