United States Army
Criminal Investigation Command

Media contact:
571-305-4041

FOR IMMEDIATE RELEASE

CID: Beware of 'Hijacked' Webcam Scams

QUANTICO, VA. (October 18, 2018) – U.S. Army Criminal Investigation Command (CID) is warning individuals to be on the lookout for cybercriminals who are attempting to blackmail victims with compromising videos.

According to Special Agents with CID's Computer Crime Investigative Unit (CCIU), the scam involves criminals claiming to have remotely accessed victim's personal computers, hijacked their webcam, and captured compromising videos of the victims and even their families. The criminals threaten to release the videos if they don't' receive a "ransom."

"This scam relies on shock value and exploits our innate human forgetfulness thus allowing cybercriminals to exploit their victim's conscience," said CCIU Director Special Agent Daniel T. Andrews. "It also capitalizes on people's fear of public embarrassment and the even more frightening prospect of ruined professional standing in the community and with employers."

Andrews further explained that the cybercriminals threaten to send the compromising video to your spouse, relatives, friends, and/or your employer; however, in exchange for a payment, the criminal will offer to destroy the video and tell no one.

"This is a scam. Do not send any payment to the blackmailer even if you receive an email specifically addressed to you," Andrews said. "Sometimes the email includes one or more of your real usernames and seems to directly target you."

Although this may be alarming, keep in mind that it's not difficult to figure out your username – as it might be part of your email address. This blackmail scam may even seem convincing when it includes one of your current or former passwords, according to agents.

CCIU agents suggest that individuals take the necessary precautions by covering the device's webcam, updating the software and hardware with the latest version, running automatic updates, turning on a firewall and using another device to change passwords.

Something as simple as covering your webcam lens with something you can't see through will prevent the camera from capturing anything but it should not be the only thing you do. Some other basic security practices are to invest in strong security software, be careful of opening links or attachments sent via email or through social media networks, use and enable two-factor authentication, and backup your data in the event you need to restore your device to its original settings.

Additionally, protect your sensitive data, log out of your profile, and never leave your device unattended.

- more -

“Always remember that everyone is a target to hackers. Remain vigilant and protect yourself,” said Christopher Grey, CID's spokesman. “If you believe you are at risk or the threat is genuine, contact your local law enforcement agency or report the incident to the Internet Crime Complaint Center at https://www.ic3.gov/default.aspx.”

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

###CID###

For more information on CID, or to report a felony-level crime, provide information concerning a crime, or if you are the victim of a crime, visit www.cid.army.mil.