United States Army
Criminal Investigation Command

Media contact:
571-305-4041

FOR IMMEDIATE RELEASE

CID: Beware of Virtual Kidnapping Scam

QUANTICO, VA. (June 26, 2018) – The U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU) is warning the Army community to be on the lookout for the "Virtual Kidnapping" hoax.

The scam occurs when an unsuspecting person receives a call and the caller immediately says, "I've kidnapped your kid. Send money or the kid dies," or some similar version of the call.

Although this is not a new scam, it recently happened to a member of the Army Family. It was quickly confirmed to be a scam because the victim called their child's school and confirmed that the child was safe in class.

"Often, victims of the virtual kidnapping fraud are chosen randomly. The person who answers the telephone is the victim, and no one has been kidnapped," CID officials said. "Sometimes criminals target a block of telephone numbers in known affluent area codes. They dial sequential numbers until the call is answered by someone they can shock into believing that their child has been kidnaped. The caller's approach is forceful, well scripted and can be very convincing."

Recipients of the call report hearing screaming in the background and desperate pleas for help, a crying child and other equally frightening sounds. The caller is loud, abrasive, abrupt, and demanding.

When the "kidnapper" uses the child's name, it will cause the victim to panic and become more compliant. But keep in mind that the caller might have found the child's name on social media or the parent might have inadvertently told the caller the child's name during the course of the call.

What to Do
If you receive a phone call from someone demanding ransom for an alleged kidnap victim, consider the following:

- In most cases, the best course of action is to hang up the phone.
- If you engage the caller, don't confirm or acknowledge your loved one's name.
- Try to slow the interaction. Request to speak with your family member directly by saying "how do I know my loved one is OK?

- Ask questions only the alleged kidnap victim would know such as the name of a pet. Avoid sharing information about yourself or your family.
- Attempt to contact the "kidnapped" victim via phone, text, or social media, and request they call back from their own cell phone.
- To buy time, repeat the caller's requests and tell them you are writing down the demand or tell the caller you need time to get things moving.
- If you suspect a real kidnapping is taking place, immediately contact the nearest FBI office, CID office, or local law enforcement agency.

Don't be a victim
To avoid becoming a victim, look for these possible indicators:
- The call does not originate from the "kidnapped" person's phone.
- The caller goes to great lengths to keep you on the line so you can't make calls or verify their claims.
- Ransom money must be paid by wire, PayPal, Moneygram or similar service.
- Ransom amount quickly decreases if the parent resists.

Remember that the fraudster relies on shock, speed and fear. Criminals know they have a small window of opportunity to extract a ransom before the victim realizes the scam or authorities become involved, officials warned.

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, 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.