Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

Email
usarmy.cciuintel@mail.mil

CCIU Web Page
http://www.cid.army.mil/701st.html#sec6

CID LOOKOUT
ON POINT FOR THE ARMY

"Do What Has To Be Done"

CPF 0003-18-CID361-9H **18 June 2018**

Virtual Kidnapping Fraud

The telephone rings. "I've kidnapped your kid. Send money or the kid dies!"

Heart stopping words for any parent. But it's not just any parent that answered the phone. It's you who answered the phone. Shock, bewilderment, panic, fear, terror are all within the expected range of emotions that jolt you into a different plane of attentiveness and suggestibility.

Recently, a member of the Army Family received just such a call. It turned out to be a hoax. A fraud. The parent called the school. The child was in class, accounted for and blissfully unaware they had been leveraged in an online fraud.

Don't be a victim!

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.

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.

While you might not be aware of this particular fraud, known as "virtual kidnapping," it's not new. The FBI was tracking kidnapping fraud as far back as 2013.

Often, victims of the fraud are chosen randomly. Let's be clear. The person who answers the telephone is the victim; no one has been snatched off the street or plucked from their classroom.

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. 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.

Caller: We have your kid. Send $2,000 immediately or he's dead.
Parent: You have Tommy? Is he OK?
Caller: Tommy! Yes, we have him. Tommy is OK for now. Listen carefully…

When the "kidnapper" uses the child's name, the parent's fear level jumps into the stratosphere. But the caller might have found the child's name on social media or the parent might have unwittingly told the caller the child's name.

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 call out your loved one's name.
- Try to slow the interaction. Request to speak with your family member directly. As, "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 contact the nearest FBI office, CID Office, or local law enforcement agency.

In the News

Virtual Kidnapping Fraud — FBI
Charges Filed in Kidnapping Scheme — United States Attorney's Office
How to Avoid Becoming a Kidnapping Fraud Victim — Washington Post
Hands Off My Data! 15 Default Privacy Settings You Should Change — Washington Post
Hands Off My Data! 15 More Default Privacy Settings You Should Change — Washington Post

Army Resources

Combatting Social Media Impersonation
Social Networking Safety Tips
Twitter Safety Tips
LinkedIn Safety Tips
Google+ Safety Tips
Facebook Safety Tips

CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide feedback.