United States Army
Criminal Investigation Command

Media contact: CID Public Affairs Office
571-305-4041

FOR IMMEDIATE RELEASE

U.S. Army CID Warn Citizens to Be Vigilant Against Internet, Digital Scammers

QUANTICO, Va. (Jan. 17, 2017) – Today in an age when most individuals communicate through their social media profiles, they should also be aware that online predators and scammers are lurking and actively stalking their next unsuspecting victim.

Now that the frantic holidays are over and Valentine's Day is fast approaching, Special Agents with the U.S. Army Criminal Investigation Command, known as CID, are expecting a different type of holiday frenzy - an increase in "Romance Scam" reports. The scam usually finds a victim claiming they are "in a relationship" with an American Soldier, when in fact their love interest is an online scammer, who hustled them out of their money and emotions.

"These perpetrators are definitely not American Soldiers, but they quite familiar with American culture," said Chris Grey, Army CID spokesperson. "The criminals, often from other countries, most notably from West African countries, are pretending to be U.S. Soldiers routinely serving in a combat zone or other overseas location.

"The perpetrators will often take on the online persona of a U.S. Soldier, who is honorably serving his country somewhere in the world or has previously served and been honorably discharged, then marry that up with some photographs of a Soldier off the Internet, and then build a false identity to begin prowling the web for victims," Grey said. "The Soldier's rank and other military details are often included in an effort to give credence to the scammer's tale."

The Army reports that several very senior officers and enlisted Soldiers throughout the Army have also had their identities stolen just to be used in these scams.

To date, there has not been one report to Army CID indicating that a U.S. Soldier has been criminally involved or suffered any financial loss as a result of these attacks. Photographs and actual names of U.S. Soldiers have been the only thing used. On the contrary, victims have lost thousands of dollars. One victim went so far as to refinance her house to help out her new beau, in the end she lost more than $70,000.

These criminals are good at what they do, and know how to get their victims emotionally involved with their scam. According to romancescam.org, the scammers set up fake social media accounts and various dating site profiles with pictures suggesting that they are from the U.S. The website went on to describe how the scammer shares tales of being a caring and loving individual who is looking for their soul mate. The scammers begin phishing for information and eventually the victim is hooked and financially invested. Once that happens, the criminals continue their ruse and then proceed to ask the victim for additional financial support by using a wide range of excuses to get the "unsuspecting love bird" to help them out of their crisis, whatever it may be.

-more-

The scam often involves carefully worded romantic requests for money from the victim to purchase computers, international telephones, military leave papers and transportation fees to be used by the fictitious “deployed Soldier” so their false relationship can continue. The scams include asking the victim to send money, often thousands of dollars at a time, to a third party address.

“I get calls every week and it is very troubling to hear these stories over and over again of people who have sent thousands of dollars to someone they have never met and sometimes have never even spoken to on the phone,” Grey said. “We cannot stress enough that people need to stop sending money to persons they meet on the Internet and claim to be in the U.S. military.”

Along with the romance-type scams, CID has received complaints from citizens worldwide that they have been the victims of other types of scams — once again where a cyber-crook is impersonating a U.S. service member. One version usually involves the sale of a vehicle; where the service member claims to be moving overseas and has to quickly sell their vehicle because they are being sent to another duty station. After sending bogus information regarding the vehicle, the seller requests the buyer do a wire transfer to a third party to complete the purchase. In reality, the entire exchange is a ruse for the crook to get the wire transfer and leave the buyer high and dry, with no vehicle.

“Another critical issue is we don't want victims walking away and thinking that a U.S. Soldier has ripped them off when in fact that Soldier is honorably serving his or her country and often not even aware that his pictures or identity have been stolen,” Grey said.

What to look for:

- DON’T EVER SEND MONEY! Be extremely suspicious if you are asked for money for transportation costs, communication fees or marriage processing and medical fees.
- If you do start an internet-based relationship with someone, check them out, research what they are telling you with someone who would know, such as a current or former service member.
- Be very suspicious if you never get to actually speak with the person on the phone or are told you cannot write or receive letters in the mail. Service members serving overseas will often have an APO or FPO mailing address. Internet or not, service members always appreciate a letter in the mail.
- Military members have an email address that end in “.mil.” If the person you are speaking with cannot sent you at least one email from a “.mil” (.mil will be the very LAST part of the address and nothing after), then there is a high probability they are not in the military.
- Many of the negative claims made about the military and the supposed lack of support and services provided to troops overseas are far from reality – check the facts.
- Be very suspicious if you are asked to send money or ship property to a third party or company. Often times the company exists, but is not part of the scam.
- Be aware of common spelling, grammatical or language errors in the emails.
- Be cognizant of foreign and regional accents that do not match the person’s story.

The U.S. has established numerous task force organizations to deal with this and other growing issues; unfortunately, the people committing these scams are using untraceable email addresses on Gmail, Yahoo, Hotmail, etc., routing accounts through numerous locations around the world, and using pay-per-hour Internet cyber cafes, which often times maintain no accountability of use. The ability of law enforcement to identify these perpetrators is very limited, so individuals must stay on the alert and be personally responsible to protect themselves.

-more-

Officials said that if you suspect that you are a victim, you should contact the authorities as soon as possible and stop all correspondence with that person immediately. They added that the scams are a grave misrepresentation of the U.S. Army and the tremendous amount of support programs and mechanisms that exist for Soldiers today, especially those serving overseas.

Where to go for help:

- **Report the theft to the Internet Crime Complaint Center (IC3) (FBI-NW3C Partnership).**
  Online: http://www.ic3.gov/default.aspx

- **Report the theft to the Federal Trade Commission.** Your report helps law enforcement officials across the United States in their investigations.
  Online: http://www.ftc.gov/idtheft
  By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261
  By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

- **Report the fraud to the Federal Trade Commission on Nigerian Scams.**
  Email: spam@uce.gov

For more information on CID, visit www.cid.army.mil.

-END-