United States Army
Criminal Investigation Command

CID LOOKOUT
ON POINT FOR THE ARMY

FOR IMMEDIATE RELEASE
Media contact: 571-305-4041

CID warns Army community about social media impersonation of Soldier accounts

QUANTICO, VA. (Feb. 2, 2018) – U.S. Army Criminal Investigation Command's (CID) Computer Crime Investigative Unit (CCIU) is once again warning Soldiers and the Army community to be on the lookout for "social media scams" where cybercriminals impersonate service members by using actual and fictitious information, not just for "trust-based relationship scams," also known as Romance Scams, but for other impersonation crimes such as sales schemes and advance fee schemes.

"By monitoring your social media identity, you can protect your Army family and your reputation," said Special Agent Daniel Andrews, CCIU director. "The criminals will use factual data from official websites and Soldiers' personal social media sites, then prey on vulnerable people's trusting nature and willingness to help the Soldier."

Frequently, CID receives notifications from individuals stating they were scammed online by someone claiming to be a Soldier, but in reality it was an online scammer who has used an unsuspected Soldier's name and available social media photos to commit a crime.

No one is immune from becoming a victim. Scammers steal the identity of senior officers, enlisted personnel and civilians. Scammers, using this information from legitimate profiles, will capitalize on the trustworthy reputation of individuals associated with the Army.

According to experts, mitigating fraudulent social media is not simple and there is no definitive way to stop criminals from using your personal data and photos. CID officials say that the ideal solution is to limit the details you provide about yourself in your social media profile. Additionally, Soldiers should take of advantage of all security and safety features and protocols offered on their social media accounts.

Another tip is to routinely search for your name on various social media platforms. Since scammers may use your photo but change the name, you should also conduct an image search of your social media profile pictures.

"Carefully scrutinize the pictures you post of yourself or are posted by others for revealing details like your name tag, unit patch and rank," Andrews said. "Creating a profile display name other than your actual name makes it more difficult for people who do not know you well to find your profile and fraudulently use your social media identity."

If you find yourself or a family member being impersonated online, CID warns that you should take immediate steps to have the fraudulent sites removed. Victims should contact the social media platform (company) and report the false profile.

-more-

Keep in mind that criminals create impersonation accounts to look just like the real account of a service member by using very similarly spelled names and replacing characters with dashes, spaces, and/or homoglyph characters. Be on the lookout for simple changes such as zeros (0) used instead of the letter "O" or a number one (1) instead of the letter "l."

"Always remember that effectively searching yourself requires creativity because of the misspelled names and other identifying information slightly different to disguise the criminal activity or just because the scammer doesn't have command of the English language," CID officials said. "Criminals will hijack photographs found on the Soldiers official and personal social media page and create a similar or identical biography."

Officials also warned that impersonations can be classified as Confidence Based/Romance Relationship, Sales Schemes or Advance Fee Schemes.

Confidence Based/Romance Relationship: Scammers defraud victims by pretending to be service members seeking romance or in need of emotional support and companionship. In these scams, cybercriminals often derive information for their fictionalized military personas from official military websites and social networking websites where military families post information about their loved ones. Scammers gather enough detailed personal information, including pictures, to concoct believable stories tailored to appeal to a victim's emotions and then lure unsuspecting victims (most often women) into sending money to help them with transportation costs, marriage processing expenses, medical fees, communication fees such as laptops and satellite telephones. They typically promise to repay the victim when they finally meet; however, once the victim stops sending money, the scammer is not heard from again.

Sales Schemes: Most frequently carried out on sites that facilitate sales of various products, scammers lure victims by offering goods well below market price. Most scams involve vehicle sales, house rentals or similar big-ticket items. The scammer advertises an item for sale, at a to-good-to-be-true price, and describes it in the broadest of terms. A person showing interest is soon contacted by the "seller" who claims to be a service member with a military unit that is being deployed abroad. The scammer uses the pending deployment to explain the need for a quick sale and, hence, the below market sales price. The scammer insists that money changes hands quickly using some untraceable and irrevocable means such as Western Union, MoneyGram or gift cards. The merchandise is never received and the scammer is not heard from again.

Advance Fee Schemes: These schemes defraud potential victims by promising big profits in exchange for help in moving large sums of money (or gold, oil, or some other commodity or contraband). Claiming to be high-ranking or well-placed government/military officials or the surviving spouse of former government leaders, the perpetrators offer to transfer significant amounts of money into the victim's bank account in exchange for a small fee. Some use photographs and biographical information of high-profile American military officials obtained from the internet. Scammers that receive payment are never heard from again.

"The Computer Crime Investigative Unit has found that the longer an imposter account is active, the greater the likelihood of misleading others," Andrews said. "Protect yourself by conducting internet searches on yourself and your family. Expediency is paramount."

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.

#Army CID#

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.