Cybercrime Prevention Flyer

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

CPF 0006-17-CID361-9H **15 May 2017**

Cyber Criminals Target Soldiers

Soldiers are being targeted by organized rings of criminals intent on extorting money from them.

U.S. Army Criminal Investigation Command (CID) receives reports each month from Soldiers who have fallen victim to online scams. Most often through social networking activities.

Social media plays a very important role in our modern lives. It helps us learn, share experiences with others and stay connected to people we care about. But social media has a dark side. A dark side where criminals operate – criminals that target Soldiers!

Soldiers, wherever they are, must protect themselves, and their good names and reputations. That includes when they are online. Soldiers who engage in dangerous online behavior place themselves at higher risk of online extortion.

Sextortion, a common online extortion scam where criminals lure Service members into engaging in online sexual activity and then demand money or favors in exchange for not publicizing embarrassing images, videos or information.

Victims of romance and sextortion scams report becoming involved in online relationships that lead to the exchange of personal, sometimes intimate, information and then receiving threats and demands.

The threat is that the Soldier's online relationship will be exposed to their chain of command or to law enforcement authorities. The demand is for money.

Even after meeting the criminal's demands, some Soldiers find themselves in a vicious, never-ending cycle of increasing demands. Some Soldiers have lost thousands of dollars to these scams. Some victims have committed suicide.

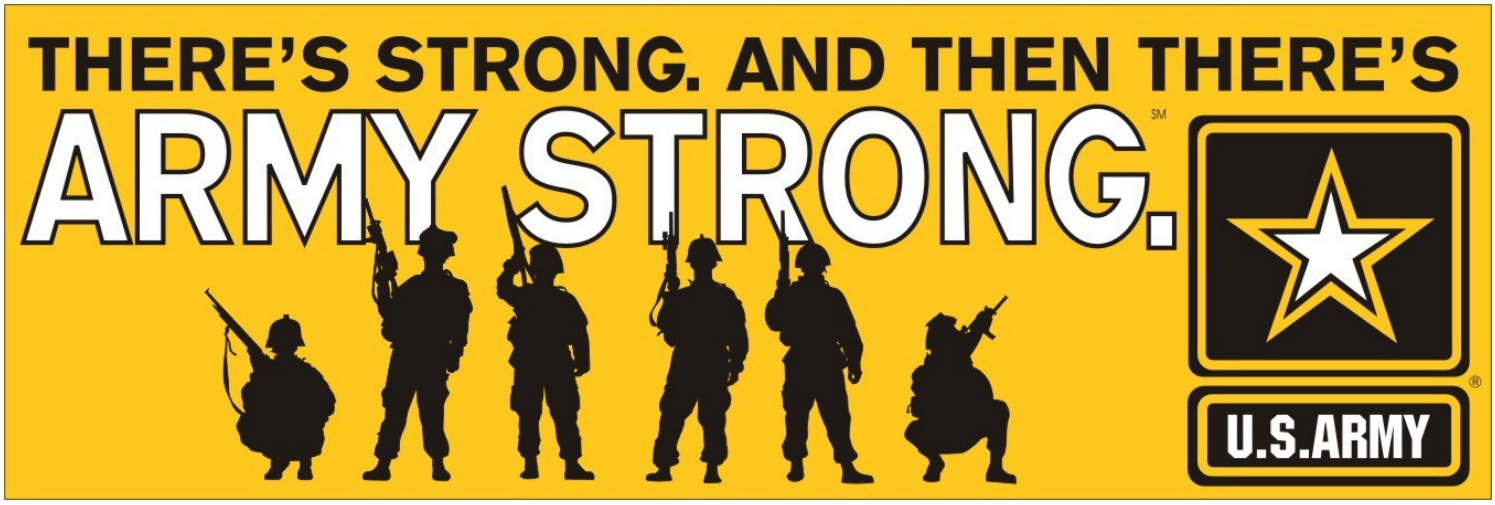
To fight against these scams, Soldiers should arm themselves with information. Learn the warning signs of fraudulent relationships and the steps to reporting a crime.

The Army has some excellent online resources that are available to everyone.

Cybercrime Prevention Flyer

Suggested Sites:

- U.S. Army Social Media—Information for the Army family
  (https://www.army.mil/socialmedia/)
- Cyber Sextortion—The nature of the crime, what you need to know and how to report it.
  (http://www.cid.army.mil/assets/docs/2can/CyberSextortion.pdf)
- Beware of Sextortion Scams—Army CID's warning message
  (https://www.army.mil/article/181694/army_cid_warns_soldiers_to_beware_of_sextortion_scams)
- Reporting Online Misconduct—
  (http://www.cid.army.mil/assets/docs/2can/OnlineMisconductFlyer.pdf)
- Defining Proper Online Conduct
  (https://www.army.mil/article/150887)



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