2CAN 0025-14-CID221-9H **9 June 2014**

Cyber Sexual Extortion ("Sextortion")

The Computer Crime Investigative Unit (CCIU) of the U.S. Army Criminal Investigation Command (USACIDC) has received reports of an increasingly-common form of criminal fraud known as cyber sexual extortion, or "sextortion." Sextortion can not only lead to embarrassment for the victim, but those who perpetrate sextortion schemes can leverage their actions for financial gain or other forms of blackmail.

In a standard sextortion scheme, a supposed attractive young female will make contact with the victim via a social networking and/or dating site. The perpetrator will send flirtatious messages and pictures and will build rapport with the victim. At some point, the victim will be asked to take part in a video session with the female, during which the subject plays video of a female conducting sexual activity and the victim is asked to do the same. Unbeknownst to the victim, the subject is recording the victim's sexual activity and, after doing so, threatens to send the recording to friends and family unless some amount between $100 and $3,000 is paid, often via Western Union or MoneyGram to overseas locations.

Victims of sextortion may be repeatedly approached for more money, all while being subject to further blackmail. Furthermore, unreported blackmail could leave a victim vulnerable to requests for sensitive information or access to U.S. Army systems and facilities. Previous sextortion schemes that have been disrupted by law enforcement were OCONUS-based and centered around areas of Asia and/or Africa, and some scammers are believed to target U.S. military service members exclusively.

If you receive "friend" requests or other unsolicited communications from unknown third parties online, be cautious. Anything said, done, or sent via the Internet may be archived and made public indefinitely. The risks of this are compounded when the person at the other end of the communication is a stranger whose pictures and profiles may not accurately represent who they are.

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

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

E-mail

CCIU Web Page

CID Cyber Lookout
On Point for the Army

Cyber Crime Alert Notice

If you have been the victim of sextortion, please do the following:

- DO NOT send money to the scammer(s). CCIU is aware of instances when scammers threatened to release videos unless a second or even third payment was made.

- DO NOT continue to correspond with the scammer(s).

- DO preserve whatever information you have from the scammer(s), such as social networking profile, email accounts used, where money was directed to be sent, etc.

- DO notify CCIU at usarmy.cciuintel@mail.mil or 571-305-4478 to report being a victim if you are a service member or civilian employee of a service branch. If you are not associated with the military, report being a victim to Homeland Security Investigations at Assistance.Victim@ice.dhs.gov.

For more information about computer security and other computer related scams, we encourage readers to visit the CCIU website to review previous cyber crime alert notices and cyber crime prevention flyers.

Additional Information:

U.S. Immigration and Customs Enforcement (ICE)

• U.S. Federal Law Enforcement Assist in Philippine Sextortion Takedown

Internet Crime Complaint Center (IC3)

• Sextortion Scam Alert