Online 'Sextortion' Scheme Targets Service Members (/xml/ahoFeatStories.asp)

NCIS provides recommendations on how to avoid becoming a victim

24 February 2015 By From Naval Criminal Investigative Service Public Affairs

While checking his Facebook account, a service member receives a friend request from a young, attractive female. The service member and female begin chatting online and subsequently exchange Skype contact information. Their online communication quickly transitions to a video chat, becoming sexual in nature...

Their online communication quickly transitions to a video chat, becoming sexual in nature and resulting in the service member engaging in online sexual acts for the female. Unknown to the service member, the female secretly is recording him.

Shortly thereafter, the female sends the service member a video file and threatens to release the video to all of his Facebook friends, family, and colleagues unless the service member sends $300.00 to the Philippines via Western Union. After the service member pays the $300, the perpetrator demands $150 more.

An increasing number of Department of the Navy (DON) and Department of Defense (DoD) personnel worldwide are falling victim to an online scheme known as sex extortion or "sextortion." Sextortion occurs when a person secretly records an online sexual interaction with a willing participant and then threatens to share the images or video with friends or family, or post the footage to an online site, unless the participant sends or deposits money.

Information from the Naval Criminal Investigative Service (NCIS) indicates that the most common DON victims are men in the E-2 or E-3 rank aged 19 to 26.

Many military service members who have fallen victim to this scheme indicated that their social media profiles lacked privacy settings or may have advertised their military affiliation, thus making them easily identifiable U.S. military-affiliated targets.

"The use of the Internet and social media has made it easy to target DON personnel," said Megan Bolduc, NCIS Division Chief, Analytical Support to Operations & Investigations. "The same general approach to luring military service members into an extortion trap has been seen in 12 NCIS field offices that have opened cases and produced criminal intelligence on the topic since August 2012."

While enlisted military men appear to be the most-targeted victims, there have been instances in which enlisted female military members have become collateral victims. For example, perpetrators of sextortion schemes have used names and photos from female Marines' Facebook profiles to create false identities. The perpetrator then uses the fraudulent identity to approach male service members online, creating a false sense of security because he believes he is communicating with a comrade who appears to be trustworthy.

Sextortion affects not only the individual victims, but also their friends, family, and colleagues, who are also at risk for exploitation. When victims allow strangers to access their social media profiles and personal data, perpetrators can gain access to critical information like their friends, relationship status, and group affiliations. As a result, subjects may use that information to identify and target additional victims.

More Featured Stories

(ftrStory.asp?id=85744)
The Battlefield Saints (ftrStory.asp?id=85744)
26 February 2015

(ftrStory.asp?id=85668)
Ghosts of Iwo Jima (ftrStory.asp?id=85668)
19 February 2015

Departments

Advancements and Promotions (dept_landing.asp?issue=3&dep=10)
Around The Fleet (dept_landing.asp?issue=3&dep=2)
Focus on Service (dept_landing.asp?issue=3&dep=1)
Health and Fitness (dept_landing.asp?issue=3&dep=7)
History and Heritage (dept_landing.asp?issue=3&dep=8)
Pay and Benefits (dept_landing.asp?issue=3&dep=12)
Talking with Sailors (dept_landing.asp?issue=3&dep=4)
Training and Education (dept_landing.asp?issue=3&dep=5)
Uniform Matters (dept_landing.asp?issue=3&dep=11)
Your Career (dept_landing.asp?issue=3&dep=6)

Sextortion incidents reported to NCIS and other law enforcement agencies indicate that perpetrators tend to follow a similar methodology when engaging a service member to participate. Understanding the process and recognizing the warning signs are critical to avoid becoming a victim. The methodology typically follows the same pattern:

* The service member is approached online via social media, usually through a Facebook friend request or message by a perpetrator posing as a single woman between the ages of 18 and 30.

* The perpetrator and the service member continue text communication for a period of time after which the perpetrator encourages the victim to transition to a video chat application, usually Skype.

* Once the conversation shifts to Skype, one of two scenarios typically takes place: The perpetrator, partially or completely undressed, immediately begins to touch herself in a sexual manner and encourages the participant to do the same or, after a brief conversation, the perpetrator persuades the service member to undress and masturbate.

* Unknown to the service member, the perpetrator is recording the sexual activities. While still engaged in the act or immediately afterward, the perpetrator reveals a video or photographs of the victim engaging in the sexual activity as evidence of his participation.

* The perpetrator then demands that the service member send money, generally via Western Union, to a designated recipient in the Philippines. If the demand is not satisfied, the perpetrator threatens to share the video or photos with the service member's family and friends, or post them to public websites, such as YouTube or DON websites.

Several warning signs should serve as red flags:

* The perpetrator's Facebook page has little or no content.
* Most of the perpetrator's friends are men affiliated with the DoD and live or reside in one particular geographic location.
* The text conversation quickly shifts to transitioning communication to Skype or a webcam application.
* The video chat begins with the perpetrator in a partial or full state of undress.
* When video chatting, the perpetrator claims the microphone is not functioning and insists she will communicate via the text feature.

Recommendations to help avoid becoming a victim of sextortion or similar criminal activity:

* Adjust social media profile settings to "private."
* Be cautious when accepting friend requests or responding to people you don't know.
* Avoid advertising or discussing affiliations with the U.S. military or U.S. government.
* Refrain from posting self-incriminating photos and videos and from engaging in online activities in which other people could post incriminating photos or videos of you.
* Do not provide personal banking or credit card information to people you don't know.
* Be proactive in identifying and reporting suspicious activity.

Service members should report all attempted sextortion, particularly any information about the individual who is attempting to exploit them, how they were approached, and the context of the interaction. If possible, service members should make note of the perpetrator's username, contact information, online friends, and other information to assist investigators in identifying the perpetrator.

"Department of the Navy personnel are an integral part of their own defense when it comes to prevention of this crime," said Special Agent Devesh Patel, a general crimes investigator in the NCIS Norfolk Field Office. "They must protect themselves from becoming easy targets and prevent others from manipulating them for money. Reporting sextortion attempts will increase service members' awareness, which will help others avoid becoming victims in the future."

If a service member or someone you know has been victimized, immediately contact your command and notify NCIS via the NCIS hotline at 1-877-579-3648 or www.ncis.navy.mil (http://www.ncis.navy.mil/pages/publicdefault.aspx). Information may also be submitted anonymously to NCIS by texting 274637 (CRIMES) or using the Tip Submit smartphone application.