TO AVOID FALLING VICTIM TO SEXTORTION:

- Adjust privacy settings of social media profiles and accounts to limit publicly available information to unknown persons.
- Exercise caution when accepting friend requests or communicating with unknown persons online.
- Avoid advertising or discussing U.S. military and/or U.S. government affiliations.
- Refrain from engaging in sexually explicit activities online, such as posting or exchanging compromising photos/videos.
- Turn off electronic devices and cover webcams when not in use.
- Safeguard your personal banking and credit card information from unknown recipients.

WHAT SHOULD YOU DO?

If you or someone you know identifies suspicious activity or that they are being targeted:

- Contact your command and your local NCIS office.
- Do not submit any payment.
- Save all messages and communications between you and the perpetrator.

REPORT IT

Local NCIS Office

www.ncis.navy.mil

Text "NCIS" + your tip info to CRIMES (274637)

"Tip Submit" Android and iPhone App (select NCIS as agency)

NCIS Hotline 1.877.579.3648

NAVAL CRIMINAL INVESTIGATIVE SERVICE

CYBERSECURITY: SEXTORTION

Web, text, and smartphone reporting is anonymous.

To learn how to submit a tip via the NCIS Text, Web,and Smartphone App Tip Line, scan the QR code with your smartphone or visit www.ncis.navy.mil.

Naval Criminal Investigative Service

Russell-Knox Building

27130 Telegraph Road

Quantico, VA 22134

If you cannot report to NCIS, notify your security officer, supervisor, or command. Per DoDD 5240.06, they are required to notify NCIS within 72 hours.

CYBERSECURITY: SEXTORTION

WHAT IS SEXTORTION?

Sextortion is a cybercrime perpetrated against unwitting victims who are approached in casual conversation via social media and then seduced into engaging in online sexual activities. After fulfilling the sexual requests, which are recorded without the victim's knowledge or consent, the victim is threatened with public exposure and embarrassment if he does not pay a specified sum of money to the perpetrator, usually through a wire transfer.

HOW DOES SEXTORTION OCCUR?

An example: 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. Unknown to the service member, the female is secretly recording the sexual act. Shortly thereafter, the female sends the service member the video file and threatens to release it to the service member's friends, family, and command unless the service member sends cash to the Philippines via Western Union. After the service member pays the initial amount, the perpetrator demands more money.

Variations on this scenario include the victim receiving phone calls and threats from the alleged father of the female or a purported law enforcement officer claiming that the female is a minor and that the filing of criminal charges is forthcoming.

WHY ARE SERVICE MEMBERS ATTRACTIVE TARGETS?

- The majority of victims are young men who are away from home and maintain an active online footprint that includes publicly viewable profile information.
- Perpetrators know service members have a steady income and are typically more financially stable than the civilian population.
- Service members must abide by the UCMJ and the standards of conduct associated with a military career.
- Service members possess security clearances, meaning they may have knowledge of military tactics, training, and other operational security items of interest to potential adversaries.

SEXTORTION IS A GROWING PROBLEM

If you've been victimized, you are not alone. Service members worldwide and across all ranks have been affected by sextortion. Since August 2012, technologically savvy perpetrators have targeted at least 160 DON service members, with more than 50 confirmed "successful" incidents of sextortion resulting in a cumulative loss of more than $45,000.

Sextortion is underreported given many service members' feelings of embarrassment and concern regarding potential consequences of their actions. Regardless, perpetrators will typically continue harassment and threats of embarrassment even if payment is made. Reporting is critical to identifying and pursuing those responsible for sextortion scams.

SEXTORTION RED FLAGS

- Unknown persons approach you online or attempt to "friend" you, even if you appear to have mutual "friends" or their "friends lists" are comprised predominantly of U.S. military members.
- The perpetrator uses poor grammar and sentence structure when exchanging messages.
- The person encourages you to engage in explicit video chat or exchange sexually explicit images almost immediately after initiating contact or "friending" you.
- A video call begins with the female in a state of undress or engaging in a sexual act.
- Communications from "law enforcement officials" occur via text message, email, or phone. Law enforcement will always notify you in person of your involvement in suspected criminal activity.