TO AVOID FALLING VICTIM TO SEXTORTION

- Refrain from engaging in sexually explicit activities online, such as posting or exchanging compromising photos/videos.
- Adjust social media privacy settings and accounts to limit information available 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.
- Turn off electronic devices and cover webcams when not in use.
- Safeguard your personal banking and credit card information from unknown recipients.
- Update antivirus software and avoid downloading apps, files, or email attachments from unverified sources.
- Trust your instincts – perpetrators are highly sophisticated and able to trick their victims into a false sense of security. If you have suspicions about the person you are communicating with, cease contact with them.

WHAT SHOULD YOU DO?

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

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

REPORT IT

Local Army CID Office

www.cid.army.mil/Submit-a-Tip/

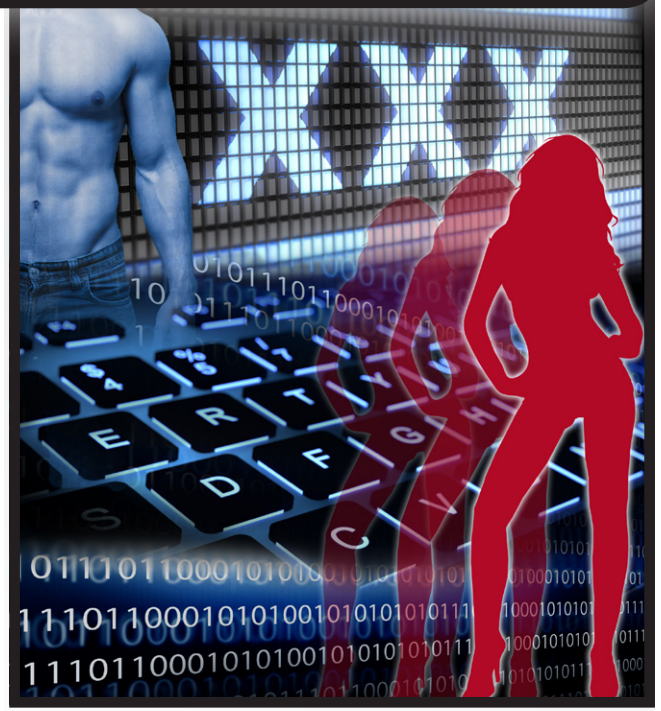
U.S. Army Criminal Investigation Command
Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134

If you cannot report possible sextortion to Army CID, notify your security officer, supervisor, or command.

HOTLINE
Department of Defense
dodig.mil/hotline | 800.424.9098

CYBERSECURITY: SEXTORTION

EXPLOITATION OF U.S. SERVICE MEMBERS



CYBERSECURITY: SEXTORTION

WHAT IS SEXTORTION?

Sexual extortion, or "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 they do not pay a specified sum of money to the perpetrator, usually through a wire transfer or subscription to pornographic websites.

HOW DOES SEXTORTION OCCUR?

An example: While checking his Facebook account, a service member received a friend request from a young, attractive female. The service member and female began chatting online and subsequently exchanged Skype contact information. Their online communication quickly transitioned to video chat, becoming sexual in nature. Unknown to the service member, the female was secretly recording the sexual act. Shortly thereafter, the female sent the service member the video file and threatened to release it to the service member's family, friends, and command unless the service member sent $500 to the Philippines via Western Union. After the service member paid the initial amount, the perpetrator demanded more money.

Variations of this scenario could include, for example, the exchange of explicit photographs leading to the victim receiving phone calls and text messages from the alleged father of the other person or a purported law enforcement officer claiming that the other person is a minor and that the filing of criminal charges is forthcoming unless the victim meets certain demands.

WHY ARE SERVICE MEMBERS ATTRACTIVE TARGETS?

- The majority of victims are young men – or in our case, junior enlisted service members – 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 are held to high 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 and services have been affected by sextortion, some having paid in excess of $11,000 to perpetrators.

Sextortion is underreported given many service members' feelings of embarrassment or concern regarding potential consequences of their actions. Regardless, perpetrators will typically continue harassment and increase monetary demands even after 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.