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

CID Cyber Lookout
On Point for the Army

"DO WHAT HAS TO BE DONE"

CPF 0002-17-CID361-9H **14 February 2017**

Cyber Sextortion

Sextortion is a serious crime where someone threatens to expose a sexual image in order to make a person do something or to seek revenge or humiliation. Cyber sextortion, as the name implies, is perpetrated across the internet. Cyber sextortion is not limited to adult victims. Victimizing youths is not an unheard of type of sextortion.

Nature of the Scam

Most often, the perpetrator (generally portrayed as a female) and the victim (generally a male) meet in a legitimate public forum such as chat sites, dating sites or any of the many social networking sites. As the online relationship develops, the victim, lured by promises of more intimacy, is asked to exchange very personal information also with intimate and sexually compromising images and videos of live sexual performances.

At some point, the relationship changes and the perpetrator demands money, threatening the victim with public and professional exposure, if not paid. There are variations of the sextortion theme. Sometimes, someone claiming to be in a position of authority, the father of the perpetrator, an attorney representing the perpetrator, or a police officer, threatens to report the victim for criminal prosecution because the perpetrator is identified as a minor.

Using the fear of public or professional exposure or the fear of criminal prosecution, the perpetrator demands money. The criminal often demands the victim forward money through a money transfer agent (e.g., Western Union, MoneyGram, Payoneer, RemitMoney) because money can be sent and received anonymously.

*Excerpt from a May 2016 Brookings Institution report entitled Sextortion: Cybersecurity, teenagers, and remote sexual assault.**

Occasionally, and especially when the victim is a minor, progressively more intimate, explicit images are demanded. Investigations have shown that often these perpetrators collect the child pornography images and trade with other child pornographers for new images.

Frequently, after terms of the extortion demand have been met, extortion demands continue and the demands escalate. The story of Ashley Reynolds, then a 14 year old high school student, describes the

* Wittes, B, (May,2015). Sextortion: Cybersecurity, teenagers, and remote sexual assault. Brookings. Retrieved February 14, 2017 from https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/

frightening process of sextortion, while the tragic suicide of Amanda Todd, a 15 year old high school student, describes the personal toll of sextortion.

What to Know

Before you send any personal information or images across the internet, before you post any personal information or images on a social networking site, before you engage in online video sessions or stream live video, think beyond the initial consequences. Anything you send that is posted to the internet, unintentionally or otherwise, will be on the internet forever.

Overcoming the embarrassment and reporting sextortion is important. Remaining silent increases the likelihood of continued harassment and extortion, and may make you susceptible to blackmail, coercion and undue influence of a foreign government.

If you are, or believe you are, the victim of cyber sextortion:

- Do not send money.
- Stop communicating with the person.
- Save all communications you have had with the person.
- Scan all computer devices for viruses and other malicious software.
- Record any telephone numbers you might have received from the person.
- Contact law enforcement authorities as soon as possible and follow their instruction.

Reporting Crimes:

- If you are a Soldier who is a sextortion victim, contact your local CID Office, the Military Police, call 1-844-ARMY-CID (844-276-9243) or email CID at Army.CID.Crime.Tips@mail.mil.
- If you are a civilian or contractor who is a sextortion victim, contact your local law enforcement agency.
- If you have any kind of a U.S. Government Security Clearance, you should report to your organization's security officer any activity that increases your susceptibility to coercion or blackmail. Failing to do so could affect your security clearance.

Additional Resources:

Sextortion—National Center for Missing & Exploited Children

Sextortion: Findings from a Survey of 1,631 Victims—Crimes Against Children Research Center

Sextortion...Victimizes George Mason Students—The Washington Post

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