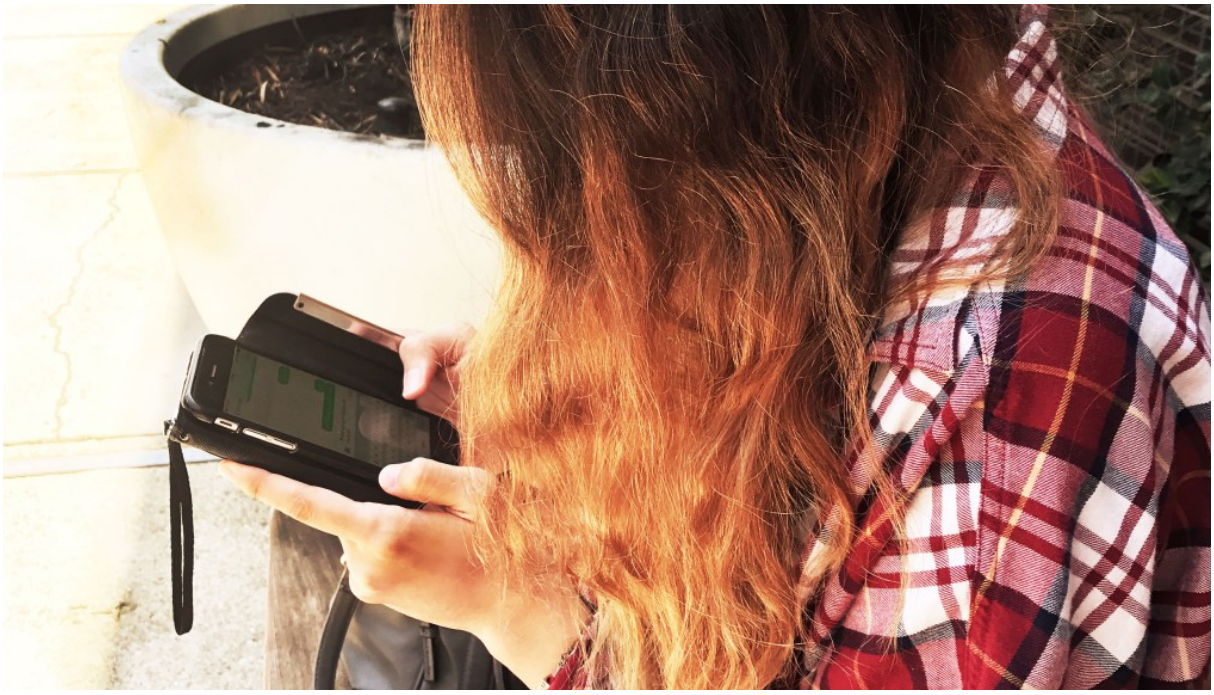
# Sextortion, a Newer Social Media Threat, is Difficult to Track

*August 16, 2017*



According to Terry Evans, a cybersecurity consultant with a background in law enforcement, many victims blame themselves. “Sextortion cases are underreported because victims are often ashamed to come forward and report the crime,” he said. Photo Credit: Nik Childers

**By Linda Childers**

Cassidy Wolf has seen the dark side of social media. Five years ago, at the age of 18, the Temecula. Calif., woman found herself at the center of a sextortion scam.

A disturbing Internet trend, the Federal Bureau of Investigation (FBI) classifies sextortion as a form of online blackmail in which explicit images are used to extort either money, additional photos or sexual favors from victims.

According to an April 2016 report to Congress by the U.S. Department of Justice, sextortion is one of the biggest online dangers to both teens and young adults. The report drew from a Brookings Institution study that called sextortion “surprisingly common.” Exact numbers are difficult to come by since sextortion isn’t a specific offense and is usually prosecuted as blackmail or extortion, but the researchers found nearly 80 cases where a “person used a computer network to extort

another into producing pornography or engaging in sexual activity." They estimate that those 80 cases involved some 3,000 victims.

In Wolf's case, Jared James Abrahams, a 19-year-old student, victimized 13 women by hacking into their webcams and recording them without their knowledge or consent. Wolf's story began with an e-mail from an unknown sender demanding that she either send naked images of herself, or agree to undress for her unknown predator via Skype. If she didn't comply, her perpetrator claimed he would post photos of her at various stages of undress that he obtained from her webcam.

Rather than give in to her predator's demands, Wolf and her family reported the threats to law enforcement.

"The FBI came to my house and after examining my computer discovered someone had hacked into one of my friend's Facebook accounts," Wolf says. "Anyone who clicked on a specific Facebook message downloaded malware that provided access to their computers, webcams and social media accounts."

In the three months it took for officials to identify the individual behind the sextortion scam, Wolf continued to receive threatening e-mails. She never responded. Finally, the FBI notified Wolf that they had identified her blackmailer as one of her former high school classmates. He was arrested and later sentenced to 18 months in prison.

"My graduating class had over 1,000 students, so I wasn't familiar with the man, but it explained how he identified many of his victims," Wolf said. "I was lucky in the sense that I had a supportive family and didn't give in to his demands."

Not all sextortion victims fare so well. Terry Evans, CEO of Cybersleuth Investigations, a Buffalo, New York-based firm that assists victims of sextortion and other cybercrimes, said many victims blame themselves.

"Sextortion cases are underreported because victims are often ashamed to come forward and report the crime," Evans said.

A cybersecurity consultant with a background in law enforcement, Evans launched his company this past April to serve as an intermediary between law enforcement and victims and to resolve matters confidentially. He also strives to educate women on how to stay safe on social media sites and to validate the identity of the person they are talking to early on to avoid being scammed.

"I've worked with victims in California and across the country who have been victims of sextortion," Evans said. "In addition to hacking computers, predators often catfish victims by using a fake online profile and hiding behind stolen photos of attractive people."

Evans called sextortion a form of victimization and sexual harassment, and said women who are pressured to provide sexually explicit photos often suffer severe psychological consequences.

"Perpetrators often demand that their sextortion victims perform humiliating and degrading acts which are used to further blackmail them and sometimes even sold on the black market," Evans said. "Women need to realize sextortion isn't their fault, even if they are duped into sending explicit photos by someone who they became involved with online."

According to the FBI, one of the most high-profile sextortion cases took place in California in 2009 when a 32-year-old man, Luis Mijangos, victimized over 230 women online, including 44 minors. After being arrested, Mijangos was sentenced to six years in prison for computer hacking and wiretapping.

Sextortion crimes aren't prosecuted in a uniform manner, Evans said. Instead, perpetrators are often charged with crimes such as blackmail and extortion, with those who prey on children typically receiving stiffer sentences than those who have victimized adults.

California Senator Connie Leyva (D-Chino) proposed a law earlier this year, SB 500, that would criminalize sextortion. The bill passed with bipartisan support in April and has moved to the Assembly. In a news release, Leyva said she hopes the new law will help state prosecutors take a firmer stance on predators who threaten to exploit victims by releasing explicit photos or demanding sex or money.