How a New Breed of Predator Is Extorting Victims Online

allure.com /story/online-predators-blackmail-sextortion-victims-explicit-images

Heather knew there were adults on the Internet who preyed on kids, and she regularly warned her own four children about the dangers of talking to strangers online. Yet the 37-year-old married mom from Phoenix never thought she would ever fall victim to a growing Internet crime known as sextortion.

The Federal Bureau of Investigation (FBI) classifies sextortion as a form of online blackmail in which explicit images are used to extort additional photos, sexual favors, and sometimes money from victims. It can involve hacking into a victim's computer or "catfishing" — where predators lure unsuspecting victims into online relationships and coerce them into sharing nude photos or videos. A 2016 report from the Brookings Institute found that sextortion is on the rise, and noted that isn't "a matter of playful consensual sexting," but rather "a form of sexual exploitation, coercion and violence."

Heather's sextortion ordeal began shortly after her family settled in Phoenix. Moving to a new town in a different state proved more stressful than she had anticipated, and she struggled to make new friends. To complicate matters, she and her husband of 11 years were going through a rough patch in their marriage. Feeling depressed and alone, Heather turned to Twitter as a social outlet.

Soon, she started connecting with other users, including Dan*, a 28-year-old entrepreneur who shared Heather's love of music.

"We were both big fans of The Who and our conversations started with banter about the band and evolved from there," Heather says. "I was upfront about being married, but Dan was smart and funny and talking with him filled a void in my life."

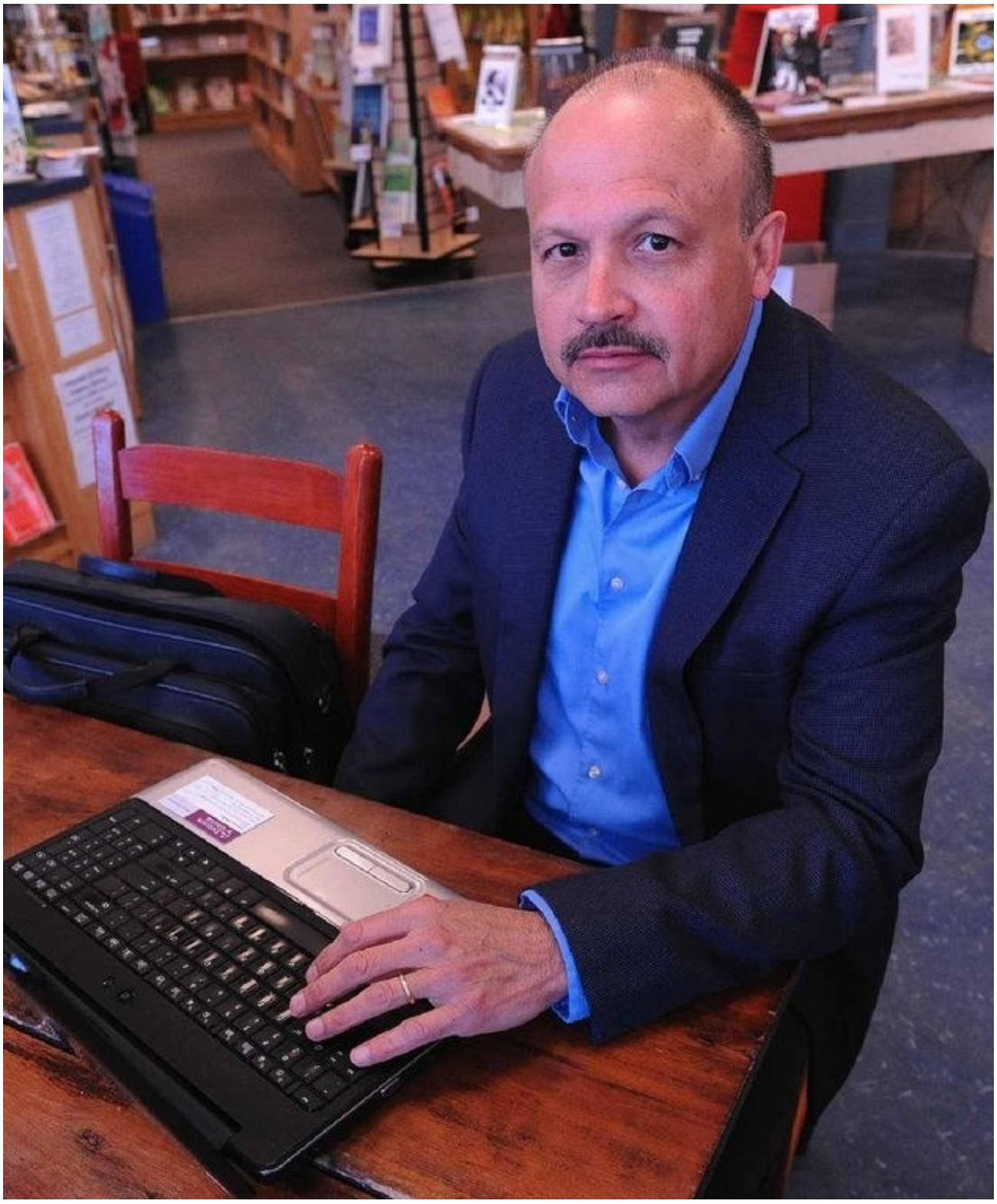
It didn't take long for Dan to move the conversation from the public Twitter timeline to communicating discreetly with Heather through private direct messages. He told Heather she was beautiful, smart and funny, and he listened to her problems. Over the course of several months, Dan went from being the perfect friend and confidante to positioning himself as the perfect lover.

"After a month of exchanging intense messaging several times a day, Dan asked me for a more revealing photo," Heather says. "By then, our conversations had gone from friendly chats to sexting."

At first she hesitated. She had never sent anyone a nude photo, but Dan was different. He made Heather feel alive and desirable in a way she hadn't felt in years. He was articulate, charming, and perhaps more importantly, he provided her with the appreciation and attention she wasn't getting at home. He also agreed to send her photos of himself. Heather later learned the images weren't actually of Dan, but of someone else.

Carefully Choosing Smart, Empathetic Targets

Terry M. Evans is president of Cybersleuth Investigations, Inc., a Buffalo, New York firm that specializes in helping victims of sextortion and other cybercrimes. He describes the techniques used to gain Heather's trust as "grooming."



Terry M. Evans

“Perpetrators like Dan often research their victims in advance so they can quickly engage them by sharing similar interests and viewpoints,” says Evans, who has a background in both law enforcement and cybersecurity. “They gain their victim’s trust by providing a sympathetic ear and by using overt attention, flattery and charm.”

While many victims blame themselves, Evans says that unlike the Nigerian prince scams where predators use broken English and implausible premises, this new breed of online predator is far savvier and more dangerous. And while you might expect to find catfishers on dating sites, Evans routinely handles cases where victims have been

approached on Facebook, Twitter, LinkedIn, Instagram, and other social media sites.

“Everyone has the need to feel loved and these online predators are very good at what they do,” Evans says. “They choose women who may be vulnerable or going through a hard time in their life.”

While a victim’s emotions may serve to cloud their judgment and lead them to explain away inconsistencies in their predator’s story, Evans stresses that in no way does that mean any victim is at fault.

As someone who was having marital problems at the time, Heather was more open to Dan's advances. Shortly after she sent Dan several photos, though, she noticed a shift in their online relationship. She suspected Dan wasn’t being completely honest with her, and sensed he was trying to manipulate her into leaving her husband.

“Dan became very insistent and tried to convince me my husband was abusive and a bad person,” Heather says. “While we had our problems, I knew he was a good person and a loving husband and father.”

As she pulled away from Dan, he became more insistent and threatened to post the intimate photos Heather had sent him, plus additional ones he had Photoshopped using her images. Heather became frightened and went to the police, but found they could offer her little in terms of help.

In the interim, Dan’s intensity escalated. He hacked into Heather’s Twitter account and began posting her images.

“Some of my friends on Twitter began pushing back and threatening to expose Dan as a catfish,” Heather says. “One friend used the information Dan had given me and traced his account.”

The truth was shocking: Dan wasn’t a handsome, successful, 28-year-old entrepreneur, but rather a married man in his mid 60s. When Heather’s friend threatened to expose him publicly, Dan backed down and removed Heather’s images. Later, she learned he had also been catfishing several other women on Twitter.

“Years ago, I was raped and I experienced the same feelings of being sexually violated,” Heather says. “Again, it was done by someone I thought I could trust, but the difference is this time, the exploitation was made public.”

A Beauty Queen Gets Hacked

In 2013, Cassidy Wolf of Temecula, California, received an email demanding that she either email nude photos of herself to an anonymous account, or agree to do whatever the email sender asked via Skype for five minutes. If she declined, the perpetrator said he would release photos of Wolf undressing that he had obtained by hacking her webcam.

Cassidy Wolf

Wolf, who was crowned Miss Teen USA in 2013, admits she was scared. But after she talked with her parents, her family decided the best course of action was to alert local law enforcement. The police informed Wolf that her webcam and computer had indeed been compromised.

“Apparently, this person had hacked one of my friend’s Facebook accounts and anyone who clicked on a specific link downloaded malware that allowed him access to their email, webcams and social media accounts," Wolf says.

Wolf’s personal computer was in her bedroom, and she learned that in order to remain safe, she should put tape over the camera.

“He had footage of me undressing in my bedroom, and he continued to email me threats, saying he would post those photos online if I didn’t do what he asked,” Wolf says. “The police advised me not to respond.”

Four months after the initial email she received, the FBI arrested Jared James Abrahams, a 19-year-old student. He was charged with hacking into the computers of multiple women and obtaining webcam footage of them in various states of undress, without their consent or knowledge. According to the U.S. State Attorney's office for the Central District of California, he may have hacked as many as 150 women.

Wolf didn’t know her perpetrator, who was sentenced to 18 months in prison, but she feels lucky she had her family’s support and didn’t give into his demands.

“I know one of the victims didn’t have anyone to talk with and tried to handle it on her own,” Wolf says. “She felt she had no choice but to give in to his demands or have her photos spread across the Internet.”

Carrie Goldberg, a Brooklyn, New York-based attorney who is considered a pioneer in the field of sexual privacy, sees many cases like Wolf’s. She says the primary motivation for perpetrators is a desire for control, and explains that victims often give in to extortion demands because they’re afraid of being shamed by their family, friends, or peers.

Carrie Goldberg

Maria Karas Photography

“Typically the ultimatum is the threat to embarrass [the victim] or expose humiliating information to the public,” she says. “Frequently the involuntary sexual act that’s demanded is something that can be performed remotely — such as taking and sending nude photographs or masturbating in front of a webcam.”

Goldberg says the material obtained is then leveraged to get additional photos or video from victims.

“For instance, the offender might have received a nude photograph voluntarily or involuntarily from the victim and then tell her he will send it to all of her Facebook friends if she doesn’t agree to send him a masturbation video,” Goldberg says. “Once he has that, he may threaten to distribute that unless she has sex with her friend on camera and so on. It is different from extortion in that money is not the objective, bur rather control. Specifically, control of someone else’s sexual behavior.”

Goldberg acknowledges that sometimes sextortion does turn into the offender demanding money in exchange for not making images public. As soon as money is demanded, however, extortion laws apply.

Evans has seen several sextortion cases go a step further, with women being asked to perform sexual acts on camera if they can’t meet the perpetrator’s demands for money. These videos are then downloaded onto the websites, including sites on the dark web, where men pay to have women perform sexual acts on camera at their request.

“Sexual exploitation has become a lucrative field, with offenders often demanding initial payments of $5,000 in order to not post images on the web or send them to a victim’s family,” Evans says. “When women can’t pay that amount, they may be asked to compensate in other ways.”

Both Evans and Goldberg have investigators who can track offenders and verify their identifies.

“Never negotiate with a criminal,” Goldberg says. “If you give in to a demand, they will continue to blackmail you and proceed to up the ante.”

The Challenge of Prosecuting Sextortion Cases

Goldberg says it’s not unusual for sextortion victims to be embarrassed about going to the police or in some cases be turned away by law enforcement officials.

“Victims give in to extortionist demands because they’re afraid of being shamed by their family, friends, or peers," Goldberg says. "Like in other sex crimes, victims of sexual extortion blame themselves and that guilt leads to repeated (and successful) attempts by the offender to blackmail.”

When the offender is a stranger, Goldberg says it can be tougher, but not impossible, to apprehend them.

“First, sextortion is drastically underreported because law enforcement lacks an understanding of how to respond to this crime," she says. "They hear the words 'Internet' or 'naked pics' or 'sex video' and don’t feel compelled to investigate further."

Goldberg says that there's been excellent work from the Department of Justice on prosecuting these cases as computer crimes.

“Historically, the cases that have resulted in prosecutions are ones where there were multiple victims,” Goldberg says. “They tend to be prolific repeat offenders.”

According to the Brookings Institute's 2016 report, out of 78 cases that fit their definition of sextortion, 13 involved more than 100 victims. And Goldberg says the average sentence in state court for such a case is 7.3 years and 29 years in federal.

Goldberg notes that sextortion charges currently depend on the particulars of individual cases.

“We presently do not have a sextortion federal law (though one is pending),” she says. “So prosecutors must use other laws that apply — extortion, computer fraud and abuse act, and cyberstalking.”

If law enforcement is reluctant to help, Goldberg says she can file what's known as a John Doe lawsuit.

“We file the case and then subpoena online service providers and social media companies for information about the offenders’ IP address, login names, et cetera,” she says. “Once we unmask the identity of the offender, we can continue with the lawsuit if that makes sense or hand it over to law enforcement.”

Protect Yourself From Sextortion

Evans and Goldberg both say no one is immune from sextortion.

“Everyone, no matter their age or gender, should be careful of striking up friendships with strangers online,” Goldberg says.

To protect yourself from being exploited online, Evans and Goldberg recommend the following.

Conduct due diligence: Evans says experienced catfishers use fake photos that often don’t show up on search engines such as Google Images and also use spoofed phone numbers that can prove harder to trace. “Today everyone has a cyber footprint, and if you’re talking to a potential romantic partner online, they should be willing to readily give out their name, occupation, and other information,” Evans says. "I work with both men and women to validate the identity of the person they are talking to online early in the relationship to ensure they are communicating with a real person and not being scammed."

Practice safety: In addition to covering your webcam with tape to ensure privacy, carefully consider whether and with whom you share explicit photos of yourself. If you do share explicit photos, you can exclude your face from them and also consider encrypting them. Keep in mind that technology can't outsmart screenshots, however. Evans adds that you should never click on an attachment from someone you don’t know. “Criminals can send links in emails or on social media that download malware onto a victim’s computer when they click on the link,” he says.

If you do find yourself the victim of sextortion, don’t panic — take the following steps:

Confide in a trusted source. “The power of the sextortion is in the shame it cultivates in the victim. Shame is the offender’s currency.” Goldberg says. “Telling a trusted friend or family member or seeking out professional help will alleviate so much of the victim’s pressure.”

Save all evidence. “Unfortunately, many victims have the knee-jerk reaction to erase the threatening emails and text messages and the exchanges they send to the offender,” Goldberg says. “It’s hugely important to save this valuable evidence and to also take screenshots of any information relating to the offender that could be fleeting — such as social media accounts, website posts, social media posts, snapchats.”

Realize you have options. In the event you are being targeted online, Evans and Goldberg says victims have options and that cases are handled discreetly. "When a client is faced with sextortion, I assist them in identifying their predator, and reporting the crime, rather than facing continued harassment and blackmail," Evans says.

While there *are* precautions you can take to avoid being blackmailed on the Internet, sextortion is never the victim's fault but rather always the fault of the perpetrator. And as online threats evolve, so too do ways of dealing with them: Remember that help is available.

**Name has been changed.*

Related:
