

THE SKINNY ON VIRTUAL KIDNAPPING

PUBLISHED
18 December 2018

CATEGORY
Kidnapping

KIDNAPPING · DECEMBER 2018

The Skinny on Virtual Kidnapping

The growth of interconnectivity – especially low or no-cost communication around the world has led to many efficiencies. For example, individuals can work on projects with team members that spread all over the world and families with a loved one serving in military can video chat using a service such as Skype or Google Hangouts. The growth, however, is not all positive. As individuals found with e-mail as it matured, scammers and other criminal perpetrators take advantage of new technologies to expand their scope of operations and to seduce unwitting individuals into sending them money. A new dark trend, virtual kidnapping, has emerged and authorities are cautioning the public as it has already ensnared some who have been left poorer and emotionally distraught at the experience.

According to the Federal Bureau of Investigation (FBI), criminals undertaking virtual kidnapping involve tricking a victim into paying a ransom for a loved one who is, indeed, not kidnapped. Rather than a traditional abduction, it is a fraud disguised as an abduction. Originally, authorities saw it primarily targeted at Spanish speaking populations in the United States who were being victimized by convicts in Mexican prisons looking to make money to either pay their way out of prison or, at least, improve their life in prison. Recently, however, it has expanded to English speaking populations in the United States and, most recently, to Mandarin speaking populations abroad and, specifically, in Calgary, Alberta (although there are reports of the same occurring in other Canadian cities).

Canadian authorities have reported that parents or loved ones of international students – specifically Chinese students – are being notified (sometimes via social media) that their loved one abroad is being held for ransom; additionally, the loved ones are being coerced by the scammers to hide out and not reply to loved ones who might be checking on them. This sometimes involves convincing the loved one that the scammers are law enforcement and threatening them with deportation if there is no cooperation with the scammer's wishes.

Outside of Canada, the Chinese Embassy in the United Kingdom is airing similar warning. Notably there, embassy officials have noted that students have been targeted and forced to take part in fake hostage videos to elicit stronger reactions from the victim's family in Chinese. In these cases, officials have reported that the scammers pose as crime fighters or embassy staff and threaten the international students to induce cooperation.

A realistic video is then sent back to the parents to increase the likelihood of compliance with ransom demands. The scammers are, it is believed, using call centers somewhere in Asia and the scammers are noted to speak in clear Mandarin which further encourages compliance with the demands of the scammers. The embassy has also noted that similar reports have been made in New Zealand, the United States, and Australia.

The FBI has developed some tips to help reduce one's likelihood of

© 2018 ThreatRate Risk Management. All Rights Reserved

falling victim to a virtual kidnapping scam (See below)



Source: https://www.deseretnews.com/article/900028900/virtual-kidnapping-scams-are-popular-and-terrifying.html

It's Sunday, Nov. 4. Fredericksburg's Hannah Stone had attended church and had breakfast with her two kids, before dropping off her 14 year-old daughter Lauren to wait for a couple of friends on Main Street. “The last thing I saw was her walking 10, 15 feet into the ice cream shop," she said. Stone hadn't driven two blocks when her phone rang. It was a strange number, but she knew her daughter's cell phone was dead so she picked it up. She heard a girl scream "mom" and the sounds of a struggle.

“I said 'Baby, Lauren, are you ok?' ” Stone said. “Then a male voice came on and said, 'We have your daughter. We took your daughter.'” The man said they were Mexican mafia, that she was being watched and that he wanted $5,000 to let her go. "My heart just stopped,” Stone said.

“My legs went numb, as I'm driving. I stop the car and went to pull over.” The next hour “was hell,” Stone said. The man, who insisted on being called sir, kept her on the phone, insisting that she talk to no one. He then coached her on how to wire money to multiple accounts.

She dropped off her son at home before heading to H-E-B to wire the money. Her husband was there and while she covered the receiver of the phone she desperately described the situation and told him to contact the police.

What she didn't know was that her daughter wasn't in any danger. The whole thing was a scam the FBI call 'virtual kidnapping,' and it’s been around for more than 10 years. "In a lot of cases they will use actors or children and they are very authentic," said Michelle Lee, FBI special agent in charge of media.

© 2018 ThreatRate Risk Management. All Rights Reserved

They don't have exact numbers because this is reported to local police along with other fraud scams and it is underreported because people are embarrassed when they find out its a scam, Lee said. Many attribute the scam to organized crime in Mexico. “Most of the schemes we have seen are focused on volume,” she said. “They're wanting to make as many phone calls as possible hoping to find a victim."

Source: http://www.keranews.org/post/fredericksburg-family-victims-virtual-kidnapping

Soundbite analytics

- 48% of kidnappings in 2017 occurred in the Americas.
- In the Americas, 97% of kidnappings were perpetrated by criminals, 3% by other armed groups.
- Only 1% of kidnappings occurred in Europe and the former Soviet Union.
- Between 2015-2017, 252 incidents of virtual kidnapping occurred in Los Angeles county alone.

FBI tips: Don’t become a victim

“The success of any type of virtual kidnapping scheme depends on speed and fear. Criminals know they only have a short time to exact a ransom before the victims unravel the scam or authorities become involved. To avoid becoming a victim, look for these possible indicators:

- Callers go to great lengths to keep you on the phone, insisting you remain on the line.
- Calls do not come from the supposed victim’s phone.
- Callers try to prevent you from contacting the “kidnapped” victim.
- Calls include demands for ransom money to be paid via wire transfer to Mexico; ransom amount demands may drop quickly.

If you receive a phone call from someone demanding a ransom for an alleged kidnap victim, the following should be considered:

- In most cases, the best course of action is to hang up the phone.
- If you do engage the caller, don’t call out your loved one’s name.
- Try to slow the situation down. Request to speak to your family member directly. Ask, “How do I know my loved one is okay?”
- Ask questions only the alleged kidnap victim would know, such as the name of a pet. Avoid sharing information about yourself or your family.
- Listen carefully to the voice of the alleged victim if they speak.
- Attempt to contact the alleged victim via phone, text, or social media, and request that they call back from their cell phone.
- To buy time, repeat the caller’s request and tell them you are writing down the demand, or tell the caller you need time to get things moving.
- Don’t agree to pay a ransom, by wire or in person. Delivering money in person can be dangerous

If you suspect a real kidnapping is taking place or you believe a ransom demand is a scheme, contact your nearest FBI office or local law enforcement immediately.”

Tips to the FBI can also be submitted online at tips.fbi.gov. All tipsters may remain anonymous.

© 2018 ThreatRate Risk Management. All Rights Reserved

Source: https://www.fbi.gov/news/stories/virtual-kidnapping

SOURCES

1 https://www.fbi.gov/news/stories/virtual-kidnapping
2 https://globalnews.ca/news/4247599/calgary-police-virtual-kidnapping-scam/
3 https://www.telegraph.co.uk/news/2018/06/08/uk-chinese-embassy-warns-students-targeted-virtual-kidnapping/
4 https://www.fbi.gov/news/stories/virtual-kidnapping
5 http://www.keranews.org/post/fredericksburg-family-victims-virtual-kidnapping.
6 https://www.deseretnews.com/article/900028900/virtual-kidnapping-scams-are-popular-and-terrifying.html

© 2018 ThreatRate Risk Management. All Rights Reserved



Risk intelligence that keeps you safe

ABOUT THREATRATE

ThreatRate helps you benchmark your risk management strategy against rapidly evolving global and local trends, with real-time, actionable analytics and insights.

For more information contact us at

info@threatrate.com

MEMBERS HAVE ACCESS TO

100+
risk-focused reports published annually

API
customised access option

Dashboards
customised dashboards and infographics

Experts
ThreatRate analysts with cross-industry depth

© 2018 ThreatRate Risk Management. All Rights Reserved

ThreatRate RISK MANAGEMENT