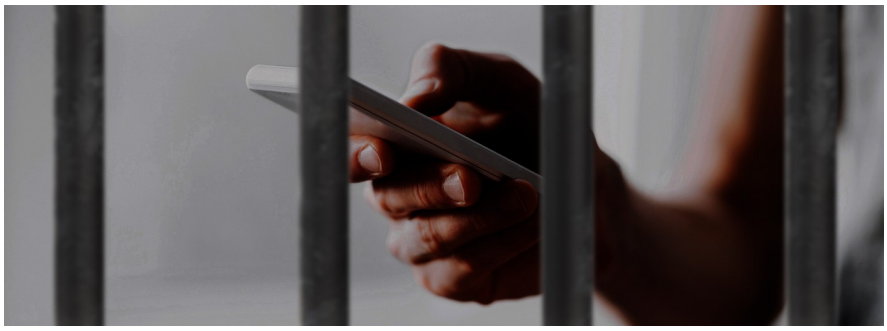
FBI

Virtual Kidnapping

A New Twist on a Frightening Scam

October 16, 2017



Law enforcement agencies have been aware of virtual kidnapping fraud for at least two decades, but a recent FBI case illustrates how this frightening scam—once limited to Mexico and Southwest border states—has evolved so that U.S. residents anywhere could be potential victims.

Although virtual kidnapping takes on many forms, it is always an extortion scheme—one that tricks victims into paying a ransom to free a loved one they believe is being threatened with violence or death. Unlike traditional abductions, virtual kidnappers have not actually kidnapped anyone. Instead, through deceptions and threats, they coerce victims to pay a quick ransom before the scheme falls apart.

Between 2013 and 2015, investigators in the FBI's Los Angeles Division were tracking virtual kidnapping calls from Mexico—almost all of these schemes originate from within Mexican prisons. The calls targeted specific individuals who were Spanish speakers. A majority of the victims were from the Los Angeles and Houston areas.

"In 2015, the calls started coming in English," said FBI Los Angeles Special Agent Erik Arbuthnot, "and something else happened: The criminals were no longer targeting specific individuals, such as doctors or just Spanish speakers. Now they were choosing various cities and cold-calling hundreds of numbers until innocent people fell for the scheme."

This was significant, Arbuthnot said, because the new tactic vastly increased the potential number of victims. In the case he was investigating, which became known as Operation Hotel Tango, more than 80 victims were identified in California, Minnesota, Idaho, and Texas. Collective losses were more than $87,000.

The incarcerated fraudsters—who typically bribe guards to acquire cell phones—would choose an affluent area such as Beverly Hills, California. They would search the Internet to learn the correct area code and telephone dialing prefix. Then, with nothing but time on their hands, they would start dialing numbers in sequence, trolling for victims.

When an unsuspecting person answered the phone, they would hear a female screaming, "Help me!" The screamer's voice was likely a recording. Instinctively, the victim might blurt out his or her child's name: "Mary, are you okay?" And then a man's voice would say something like, "We have Mary. She's in a truck. We are holding her hostage. You need to pay a ransom and you need to do it now or we are going to cut off her fingers."

Most of the time, Arbuthnot said, "the intended victims quickly learned that 'Mary' was at home or at school, or they sensed the scam and hung up. This fraud only worked when people picked up the phone, they had a daughter, and she was not home," he explained. "But if you are making hundreds of calls, the crime will eventually work."

The scammers attempt to keep victims on the phone so they can't verify their loved ones' whereabouts or contact law enforcement. The callers are always in a hurry, and the ransom demand is usually a wire payment to Mexico of $2,000 or less, because there are legal restrictions for wiring larger amounts across the border.

Although victims were typically instructed to wire ransom payments, two individuals in Houston were coerced into paying larger amounts—totaling approximately $28,000—that could not be wired. The victims were directed to make money drops, and they believed they were being watched as they were directed to the assigned location. When the drops were made—in specified trash cans—a Houston woman, 34-year-old Yanette Rodriguez Acosta, was waiting to pick up the ransom money. After taking her portion of the payment, Acosta wired the rest in small amounts to several individuals in Mexico to transfer to the Mexican prisoner believed to be running the virtual kidnapping scheme.

Acosta was taken into custody for her involvement in the scam, and in July 2017, a federal grand jury in Houston returned a 10-count indictment against her. Among the charges were wire fraud and money laundering.

Arbuthnot noted that the Mexican prisoners who carry out virtual kidnappings use the ransom money to pay bribes and to make their lives behind bars easier. "And sometimes they use the money to buy their way out of jail. That's the ultimate goal."

He added that virtual kidnapping cases are difficult to investigate and prosecute because almost all of the subjects are in Mexico, and the money is wired out of the country and can be difficult to trace. The charges against Acosta represent the first federal indictment in a virtual kidnapping case. In addition, many victims do not report the crime, either because they are embarrassed, afraid, or because they don't consider the financial loss to be significant. Regardless, Arbuthnot said, "victims of virtual kidnapping scams are traumatized by these events, because at the time, they believe that a loved one has been kidnapped and is in real danger."

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.