Don't Become a Victim of Virtual Kidnapping!

Need to know

A virtual kidnapping scam may take on one of several different forms, but it is always designed to trick victims into paying a ransom to free a loved one from what they believe to be a fear of violence or death. According to the FBI, between 2013 and 2015, investigators in the FBI's Los Angeles Division were tracking these virtual kidnapping calls from Mexico, almost all of which originated from Mexican prisons. **These scams appeared to target Spanish-speaking victims**, the majority of which were from the Los Angeles and Houston areas. Around 2015, the calls began coming in English, and fraudsters were cold-calling hundreds of numbers until someone fell prey.

The FBI warns that the fraudsters are always in a hurry, and that it usually involved a wire payment to Mexico. They also note that wires are typically done in small amounts because there are legal restrictions for wiring larger amounts across the border. They may also ask for prepaid cards or request cash payments in person, such as a money drop at a specified location. The fraudster might warn that you are being watched to avoid you going to the police. Once you have made one payment, they may phone back and demand more. They often allege to be part of a Mexican drug cartel or pretend to be a corrupt law enforcement agent and threaten harm if you don't agree to pay.

"We have your son/daughter/grandchild. We are part of a Mexican drug cartel..."

"You must pay a ransom or I will cut him/kill him."

"We are holding her hostage and will sell her if you don't pay".

The scam has moved closer to home, and in February 2018, the Ventura Police Department warned of an increase in reported cases targeting the city of Ventura. More recently, the Santa Barbara County Sheriff's office warned of an uptick in virtual kidnapping scams in our communities as fraudsters target wealthier zip codes, such as Santa Barbara County, San Luis Obispo County, and Beverly Hills, in their cold-calling efforts.

They are not as easy to spot as you might think!

Scams are becoming more and more sophisticated, and the crooks may use social media or technology to gather information and track the whereabouts of the supposed kidnap victim to add credibility to their claims. They listen for information you provide in response to their calls and will use it in the calls to make them more realistic. Technology makes it easier for scammers to fake caller ID.

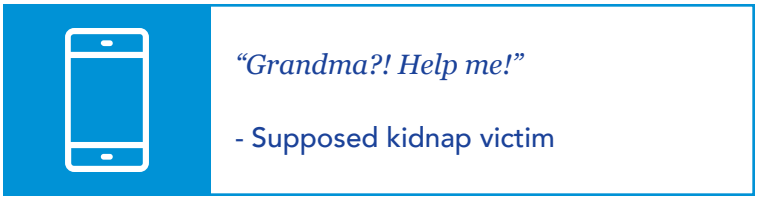
It is often difficult to think clearly to identify the red flags due to terror and fear that their loved one is in danger and that they must pay money to ensure their safe release!

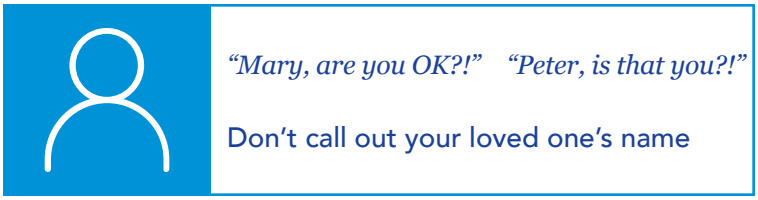
The success of any type of virtual kidnapping scheme depends on speed and fear. Criminals know they only have a short time to extract a ransom before the victims unravel the scam or authorities become involved.

How to Avoid Becoming a Victim

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 until the money is sent. **They may demand that you place your phone on speaker and in your pocket while you go to the bank.**
- They may threaten / dissuade you from calling to verify with loved ones or calling law enforcement.
- They are always in a hurry, and may make multiple, excessive calls.
- Calls do not come from the supposed victim's phone.
- May start with a person screaming for help, after which, callers try to prevent you from contacting the "kidnapped" victim.





- Calls include demands for ransom money to be paid via wire transfer to Mexico, prepaid card, or money drops.
- They may decrease the ransom request at the first sign of resistance to the amount.
- The fraudster may claim you are being watched and warn you not to go to the police.

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**.
- **Attempt to contact the alleged victim via phone, text, or social media**, and request that they call back from their cell phone. Start a group text with family and friends.
- If you do engage the caller, **don't call out your loved one's name**.
- Request to speak to your family member directly, without using names.
  Ask, *"How do I know my loved one is okay?"* or *"May I speak him/her?"*
- **Ask questions only the alleged kidnapped victim would know**, such as the name of a pet or something else not readily available through social media or online. Avoid sharing information about yourself or your family.
- **Listen carefully to the voice of the alleged victim if they speak.** In these scams, typically the supposed kidnap victim will scream or whisper to disguise their voice.
  - Does it appear to be a recording?
  - Is a script being read?
  - Is it improvised?
- Buy time to reach out to the alleged victim by repeating the caller's request. Tell them you are writing down the demand, or tell the caller you need time to collect the money. Ask *"If I can't get you the money right away, how do I let you know?"*
- 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 (**Los Angeles office: 310-477-6565**) or local law enforcement immediately. Tips to the FBI can also be submitted online at **tips.fbi.gov**. All tipsters may remain anonymous.

Virtual Kidnapping

This is to warn you of an increasing scam known as a "virtual kidnapping". The scam relies on fear, and you may be pressured to act quickly to avoid contacting the supposed loved one who is said to be in danger.

- ☐ Are you on the phone with someone?
- ☐ Are you or a loved one being threatened / extorted?
- ☐ Were you asked for a ransom?
- ☐ Do you need help?
- ☐ Would you like me to call the police?
- ☐ Is there anyone else I can call for you? If so, who?

Name: _____

Number: _____

Date of the call: _____

Time it began: _____

Time it ended: _____

Call recipient: _____

Caller ID #: _____

Threat (exact words): _____

_____

_____

Other observations: _____

_____

_____

Virtual Kidnapping

This is to warn you of an increasing scam known as a "virtual kidnapping". The scam relies on fear, and you may be pressured to act quickly to avoid contacting the supposed loved one who is said to be in danger.

- ☐ Are you on the phone with someone?
- ☐ Are you or a loved one being threatened / extorted?
- ☐ Were you asked for a ransom?
- ☐ Do you need help?
- ☐ Would you like me to call the police?
- ☐ Is there anyone else I can call for you? If so, who?

Name: _____

Number: _____

Date of the call: _____

Time it began: _____

Time it ended: _____

Call recipient: _____

Caller ID #: _____

Threat (exact words): _____

_____

_____

Other observations: _____

_____

_____

Virtual Kidnapping

This is to warn you of an increasing scam known as a "virtual kidnapping". The scam relies on fear, and you may be pressured to act quickly to avoid contacting the supposed loved one who is said to be in danger.

- ☐ Are you on the phone with someone?
- ☐ Are you or a loved one being threatened / extorted?
- ☐ Were you asked for a ransom?
- ☐ Do you need help?
- ☐ Would you like me to call the police?
- ☐ Is there anyone else I can call for you? If so, who?

Name: _____

Number: _____

Date of the call: _____

Time it began: _____

Time it ended: _____

Call recipient: _____

Caller ID #: _____

Threat (exact words): _____

_____

_____

Other observations: _____

_____

_____