ConnectSafely

QUICK-GUIDE FOR FAMILIES

Virtual Kidnapping Scams

What is a virtual kidnapping scam?

A virtual kidnapping scam is a criminal attempt to extort money from victims by convincing them that a loved one has been kidnapped and that they must pay a ransom to secure their safety. The scam can be terrifying for those who fall victim to it.

Scammers may clone a friend or family member's phone number to make it seem like the call is coming from their phone, or the call could come from an unfamiliar number. It may start with what appears to be a loved one crying or screaming. Some criminals are now using AI to clone the voice of the supposed kidnapping victim to make the call even more convincing.

While real kidnappings are rare, at least in the United States, virtual kidnappings are on the rise.

Detecting the scam

Stay calm if you suspect you have been contacted by someone running this scam. The scammer uses fear and deception to destabilize their victims and convince them that the threat is real. Even if you know such scams exist, receiving a call from someone claiming they might hurt someone you love can be extremely unnerving.

The scammer might begin the call pretending to be someone from law enforcement or another authority figure before pivoting to their threat.

Prevention & Preparation

- Discuss virtual kidnapping with family members and loved ones now and prior to any travel.
- Avoid posting your real-time location or travel plans online.
- Try to avoid posting your phone number or a recording of your voice online.
- With their permission, reciprocally share your cell phone location with loved ones using Google Maps, iCloud, or another legitimate tracking service.
- Say nothing or as little as possible to spam callers so they can't record a sample of your voice.
- Avoid sharing personal details with people you don't know. Scammers use this information to make their claims more convincing.
- If possible, make a mental or written note of what loved ones are wearing when they leave the house and where they are going.

Detecting the scam (Cont'd)

Do not give them any personally identifying information, like your name, your location, or your loved one's name or information. If you suspect you have received a scam call, the FBI advises hanging up.

If you decide to remain on the line and another person is around, tell them to call 911 while you're talking to the scammer. If you're alone, discreetly call 911 from another phone, if possible, and let the 911 operator hear the call through your cellphone's speaker. You can briefly put the scammer on mute to speak with the 911 operator, who may ask you for your loved one's phone number.

As soon as you can, try to reach your loved one by calling them or having someone else call their phone or check their location if they've shared it with you. You can also try to reach someone who would be able to confirm your loved one's safety.

Ask to speak with the person they claim to have kidnapped. If they pass you to another person or perhaps an AI bot, ask them a question that only your loved one would know the answer to. To protect themselves from scams like this, some families create code words that only family members would know.

The scammer might refuse to put the person on the phone but still claim to be holding them hostage. If so, ask the alleged kidnapper to describe your loved one's appearance or clothing (if you know what they were wearing that day).

For more information, visit ConnectSafely.org

To protect themselves from scams, some families create code words that only family members would know.

About ConnectSafely

ConnectSafely is a Silicon Valley, California-based nonprofit organization dedicated to educating users of connected technology about safety, privacy and security. We publish research-based safety tips, parents' guidebooks, advice, news and commentary on all aspects of tech use and policy.