FEDERAL BUREAU OF INVESTIGATION

OFFICE OF PRIVATE SECTOR

#VIRTUAL KIDNAPPING

VIRTUAL KIDNAPPING, or virtual kidnapping for ransom, is a coercive telephonic scheme used to extort ransom payments from victims. The victims are contacted, via telephone, and tricked into believing their loved one has been kidnapped, is at risk of being kidnapped, or is in imminent danger. By using shocking threats and sometimes using a victim's screaming voice in the background, the perpetrators pressure victims into immediately paying a ransom. If the threats do not work and because the criminals do not want to spend time on negotiations, they may quickly lower the ransom amounts. Regardless, the criminals want to receive the ransom before the scheme can be discovered.

THE SCHEME

Virtual kidnapping usually targets the "victim's" family by telephone. For example, when the unsuspecting family member answers the phone, they hear a screaming voice asking for help. The screamer's voice is likely a recording of another scammer, pretending to be a loved one, who has been "kidnapped." Upon hearing the screaming of someone the victim believes to be a loved one—a child, parent, or spouse— the family member may blurt out the loved one's name, such as, "Billy, is that you!?" Now the scammers have a name to weave into the story of a loved one being held ransom. As a proof of life, the scammers may use three-way calling to put the "victim" on the phone with their family, but then disconnect the call and threaten extreme violence upon the kidnapped victim unless the ransom is paid. The scammers demand immediate payment of ransom, or the loved one will be killed, tortured, ears or fingers cut off, or other shocking threats.

The scheme only works when someone answers the phone, is so terrified by the thought of their loved one in danger that they believe the scam and give the scammers information to work with.

The scammers will attempt to keep victim's family member on the phone to both avoid verifying their loved ones' whereabouts or alerting the police. Because the criminals want to receive the ransom before the scheme can be discovered, they may demand a wire payment of a reasonable amount, such as a few thousand dollars; additionally, there are legal restrictions for wiring large sums of money. If the family member hesitates to pay the ransom, the scammers may quickly decrease the ransom demand, to avoid prolonging the negotiations. However, if the family member pays the ransom, the criminals will likely request additional ransom payments.

If the virtual kidnapping is an international scheme, the victim's family may be told they are being watched and monitored by violent persons. Even though the scammers have no physical control, they may try and isolate the victim's family by convincing them to check into a hotel or a location in which the kidnapped victim previously resided. The scammers then contact the victim's family by gaining access to the victim's phone or asking the victim for telephone numbers and attempt to extort money from the family.

SCAM INDICATORS:

- Scammers may direct you to download a messaging application, for further communication;
- Scammers may try and keep you on the phone, with increasing threats or other Urgent needs;
- Calls do not come from a recognized telephone number;
- Scammers try to avoid having you call the kidnapped victim's phone;
- Scammers demand ransom be paid via wire transfer, quick money "drops."

WHAT TO DO:

- Before hanging up the phone, evaluate the legitimacy of the kidnapping by assessing the situation, closely listen to the caller's statements without providing details or identifying information;
- Control your emotions; slow the conversation down, and demand to speak with your loved one;
- Ask questions only the alleged kidnap victim may know, such as the name of a pet, do not share personal information;
- Listen carefully to the voice of the alleged victim if you speak to him or her;
- Attempt to contact the alleged victim via cell phone or text and request a call back from their own cell phone and;
- To buy time, repeat the caller's request, ask the caller to repeat, tell them you are writing things down, and explain it will take time to get things in action.
- Do not advertise the missing person on any social media platforms.

If you suspect a real kidnapping is taking place, or if you believe the ransom demand is a scheme, contact your nearest police department or FBI office at **1-800-CALL-FBI (1-800-225-5324)**.

You can email FBI at:
www.fbi.gov/contact-us

THE SCAMMERS

Scammers often work in an organized group. They use the Internet, social media, and other resources to their advantage, often dialing numbers in sequence to find and troll victims. It is likely that virtual kidnapping schemes will increase in sophistication as scammers exploit technology, such as caller ID spoofing and social media. Caller ID spoofing occurs when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Do not advertise the missing person on any social media sites, as additional and separate scammers may respond to reports of a missing person and capitalize on a family who is already in a vulnerable position.