FAMILY SECURITY

Virtual Kidnapping: A Family Protocol Agreed Before the Call

In April the director of the CICPC, Douglas Rico, described a virtual kidnapping pattern aimed at people who sell through Facebook Marketplace or Instagram shops. The criminals phone the seller, say they are being watched, pressure them to go somewhere isolated and ask for a relative's number. Then they call that relative to say the person has been kidnapped. According to Rico, nobody had been kidnapped: once the family transferred the money, the callers hung up. In one case under investigation, the CICPC counted more than 30 victims.

The April warning was reported in El Diario on 16 April 2026.
https://eldiario.com/2026/04/16/cicpc-secuestro-virtual/

In May, La Patilla reported, the CICPC announced it had dismantled a network whose main caller operated from a prison in Bogotá. It mainly used Marketplace to find victims and demanded urgent transfers, first to Colombian accounts and then to Venezuelan banks. In September the CICPC warned again about virtual kidnapping calls made from abroad, about forged CICPC summonses and about calls that display the real numbers of banks, phone companies or police forces.

Why the Call Sounds Believable

In the September warning, a CICPC digital forensics specialist said scammers profile their victims in advance and press on three levers: they simulate authority, create urgency and fake familiarity by quoting real personal and financial data that has already leaked. In June the CICPC also said audio and video forgeries (deepfakes) are among the mechanisms its investigators are watching most closely. None of the reports cited here says a cloned voice was used in these cases. Even so, a voice that sounds familiar should not count as proof.

The warning about fake summonses and spoofed numbers was reported in El Diario on 15 September 2026.
https://eldiario.com/2026/09/15/extorsiones-cicpc/

Data of that kind is in circulation. VE Sin Filtro reviewed a sample of the February 2026 Cashea leak and found customers' full names, cédula numbers, phone numbers and purchase details; Cashea said accounts had not been breached and that access and passwords were protected. In 2025, according to Bloomberg Línea, the same organisation reported that names, ID numbers, locations and phone numbers of 3.2 million Movistar customers in Venezuela had been posted on an online forum, and a company representative said the matter was under investigation. Nobody can tell

where each detail a caller quotes comes from, and you do not need to: the protocol has to work even if the caller knows your cédula number.

VE Sin Filtro's analysis of the Cashea leak was reported by Finanzas Digital on 23 February 2026.
https://finanzasdigital.com/ve-sin-filtro-filtracion-cashea/

Agree the Protocol While Everyone Is Calm

- Agree with your family on a verification question whose answer is not on social media, in leaks or on documents: not a cédula number, a birthday or the name of a pet that appears in photos.
- Decide who calls whom, and on which second channel: another number, another relative, the office or a trusted neighbour.
- Set the rule that no money moves while the call lasts: hang up, call the person on a number you already have and confirm before any transfer.
- If everyone agrees, turn on location sharing between the adults in the family and practise checking it, knowing that a phone that is off or has no signal confirms nothing.
- Keep at hand the address of the nearest CICPC office and of its anti-extortion division, and never lend your bank account to anyone: the CICPC warns that these networks use third parties' accounts.

If you sell online, the agreement covers meetings too: tell someone the place and time, choose a busy spot and agree a short check-in message. If a stranger calls to say you are being watched, do not go where you are told: head towards people or security staff. In September the CICPC advised hanging up, not confirming where you are and contacting your family and the authorities. Your physical safety comes before any instruction from the caller.

Less Exposure, and Accounts That Are Harder to Take Over

In April the CICPC recommended setting social media accounts to private and not posting locations, relatives or signs of wealth. Check which sale listings show your personal number and consider a separate number for selling. Look for posts that let someone rebuild your routines: the school, the gym, the time you leave work. In June the CICPC warned that once criminals take over a WhatsApp or Telegram account they ask the victim's contacts for emergency transfers, and it recommended two-step verification in every messaging app.

How Executive Digital Protection Sets It Up

With the consent of each adult in the family, and of parents where there are minors, we write the protocol with them and rehearse it with a simulated call that everyone knows is an exercise. We

review private exposure: listings, profiles and posts that show phone numbers, relatives or routines, and we prepare takedown requests where the platform allows them. We set up two-step verification and recovery for each person’s messaging accounts on their own phone, without collecting their passwords. Depending on the plan, leak monitoring warns if it finds the family’s details in a new leak, which is the moment to go over the protocol again.

> *A protocol reduces pressure and gives clear steps. It cannot stop anyone from calling, and it cannot guarantee that a platform removes content or that leaked data disappears. Under a threat, physical safety comes first, then a report to the CICPC. We are not a police or negotiation service.*

A Check You Can Run

Sit for a few minutes with each adult in the family while they open WhatsApp on their own phone and go to Settings, Account, Two-step verification. If it is off, they turn it on and create the password themselves (WhatsApp is replacing the old six-digit PIN with a password), add an email address they can reach and look at the trusted devices listed there. The password goes into their own password manager, not to you. When they finish, ask them to say, without looking it up, which second-channel number the family protocol uses. The menu path can vary slightly between Android and iPhone.

Supporting guidance: WhatsApp’s instructions for two-step verification.
https://faq.whatsapp.com/1920866721452534/?cms_platform=android

Continue with: Protecting Your Family Does Not Require Reading Every Conversation.
https://systems.kavaliero.com/en/blog/protecting-your-family-without-monitoring-every-conversation

For help with this work, see the scope of Executive Digital Protection.
https://systems.kavaliero.com/en/services/executive-security