SEGURIDAD FAMILIAR

Secuestro Virtual: Un Protocolo Familiar Acordado Antes de la Llamada

En abril, el director del CICPC, Douglas Rico, describió una modalidad de secuestro virtual dirigida a personas que venden por Marketplace de Facebook o en tiendas de Instagram. Los delincuentes llaman al vendedor, le dicen que está vigilado, lo presionan para ir a un lugar solitario y le piden el número de un familiar. Después llaman a ese familiar para decirle que la persona está secuestrada. Según Rico, nadie estaba secuestrado: cuando la familia transfería, colgaban. En un caso que investigaba, el CICPC contaba más de 30 víctimas.

La alerta de abril fue recogida en la nota de El Diario del 16 de abril de 2026.
https://eldiario.com/2026/04/16/cicpc-secuestro-virtual/

En mayo, según La Patilla, el CICPC anunció que había desmantelado una red cuyo principal llamador operaba desde una cárcel de Bogotá. Usaba sobre todo Marketplace para atraer víctimas y exigía transferencias urgentes a cuentas en Colombia y luego en bancos venezolanos. En septiembre, el organismo alertó otra vez sobre secuestros virtuales con llamadas desde el extranjero, sobre falsas citaciones del CICPC y sobre llamadas que muestran en pantalla los números reales de bancos, operadoras telefónicas o cuerpos policiales.

Por Qué la Llamada Suena Creíble

En la alerta de septiembre, un especialista en forense digital del CICPC explicó que los estafadores perfilan antes a la víctima y la presionan con tres recursos: simulan autoridad, crean urgencia y fingen familiaridad citando datos personales y financieros reales que ya se filtraron. En junio, el CICPC también dijo que las falsificaciones de audio y video (deepfakes) están entre los mecanismos que más atención reciben de sus investigadores. Ninguno de los reportes citados aquí dice que se haya usado una voz clonada en estos casos. Aun así, una voz parecida no debería contar como prueba.

La alerta sobre citaciones falsas y números suplantados fue recogida en la nota de El Diario del 15 de septiembre de 2026.
https://eldiario.com/2026/09/15/extorsiones-cicpc/

Hay datos de ese tipo en circulación. VE Sin Filtro revisó una muestra de la filtración de Cashea de febrero de 2026 y encontró nombre completo, cédula, teléfono y detalle de compras de clientes; Cashea afirmó que las cuentas no fueron vulneradas y que los accesos y contraseñas están protegidos. En 2025, según Bloomberg Línea, la misma organización reportó que nombres,

números de identidad, ubicaciones y teléfonos de 3,2 millones de clientes de Movistar en Venezuela se publicaron en un foro en línea, y un representante de la empresa dijo que el asunto estaba bajo investigación. Nadie puede saber de dónde sale cada dato que menciona quien llama, y no hace falta: el protocolo tiene que funcionar aunque el estafador sepa tu cédula.

El análisis de VE Sin Filtro sobre Cashea fue reseñado por Finanzas Digital el 23 de febrero de 2026.
https://finanzasdigital.com/ve-sin-filtro-filtracion-cashea/

El Protocolo Se Acuerda en Calma

- Acuerda con tu familia una pregunta de verificación cuya respuesta no aparezca en redes, filtraciones ni documentos: ni la cédula, ni la fecha de nacimiento, ni el nombre de la mascota que sale en las fotos.
- Define quién llama a quién y por qué segundo canal: otro número, otro familiar, la oficina o un vecino de confianza.
- Fija la regla de que ningún dinero se mueve mientras dure la llamada: se cuelga, se llama a la persona a un número que ya conoces y se confirma antes de cualquier transferencia.
- Si todos están de acuerdo, activen la ubicación compartida entre los adultos de la familia y practiquen consultarla, sabiendo que un teléfono apagado o sin señal no confirma nada.
- Ten a mano la dirección de la delegación del CICPC más cercana y de su División contra Extorsión, y no prestes tu cuenta bancaria a nadie: el CICPC advierte que estas redes usan cuentas de terceros.

Si vendes por internet, el acuerdo incluye las citas: avisa a alguien del lugar y la hora, escoge un sitio con gente y acuerda un mensaje corto de confirmación. Si un desconocido llama para decirte que te están vigilando, no vayas hacia donde te indica: acércate a otras personas o a personal de seguridad. En septiembre, el CICPC recomendó cortar la llamada, no confirmar dónde estás y comunicarte con tu familia y con las autoridades. Tu seguridad física va antes que cualquier instrucción de quien llama.

Menos Exposición y Cuentas Más Difíciles de Tomar

En abril, el CICPC recomendó poner las redes en modo privado y no publicar ubicaciones, familiares ni nivel económico. Revisa qué anuncios de venta muestran tu número personal y considera usar un número aparte para vender. Busca también publicaciones que permitan reconstruir rutinas: el colegio, el gimnasio, la hora de salida del trabajo. En junio, el CICPC advirtió que, cuando toman una cuenta de WhatsApp o Telegram, los delincuentes piden transferencias de emergencia a los contactos, y recomendó activar la verificación en dos pasos en todas las

aplicaciones de mensajería.

Cómo lo Prepara Blindaje Ejecutivo

Con el consentimiento de cada adulto de la familia, y de los padres cuando hay menores, redactamos el protocolo con ellos y lo ensayamos con una llamada simulada que todos saben que es un ejercicio. Revisamos la exposición privada: anuncios, perfiles y publicaciones que muestran teléfonos, familiares o rutinas, y preparamos solicitudes de retiro donde la plataforma lo permite. Configuramos la verificación en dos pasos y la recuperación de las cuentas de mensajería en el teléfono de cada persona, sin recoger sus contraseñas. Según el plan, el monitoreo de filtraciones avisa si encuentra datos de la familia en una filtración nueva, que es el momento de repasar el protocolo.

> *Un protocolo reduce la presión y da pasos claros. No impide que alguien llame, ni garantiza que una plataforma retire contenido o que un dato filtrado desaparezca. Ante una amenaza, la prioridad es la seguridad física y luego la denuncia ante el CICPC. No somos un servicio policial ni de negociación.*

Una Comprobación Concreta

Siéntate unos minutos con cada adulto de la familia mientras abre WhatsApp en su propio teléfono y entra en Ajustes, Cuenta, Verificación en dos pasos. Si está desactivada, la persona la activa y crea la contraseña por su cuenta (WhatsApp está sustituyendo el antiguo PIN de seis dígitos por una contraseña), añade un correo al que tenga acceso y revisa los dispositivos de confianza que aparecen ahí. La contraseña va a su propio gestor de contraseñas, no a ti. Al terminar, pídele que diga sin buscarlo qué número de segundo canal usa el protocolo familiar. La ruta del menú puede variar un poco entre Android y iPhone.

Documentación de apoyo: Instrucciones de WhatsApp para la verificación en dos pasos.
https://faq.whatsapp.com/1920866721452534/?cms_platform=android

Para seguir leyendo: Proteger a Tu Familia No Exige Vigilar Cada Conversación.
https://systems.kavaliero.com/blog/proteger-a-tu-familia-sin-vigilarla

Si necesitas ayuda con este trabajo, consulta el alcance de Blindaje Ejecutivo.
https://systems.kavaliero.com/soluciones/blindaje-digital