CajaCaracas
Casa de Bolsa

Unidad de Administración de Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo, Financiamiento a la Proliferación de Armas de Destrucción Masiva y Otros Ilícitos
(UARLC / FT /FPADM)

BOLETÍN INFORMATIVO

NOVIEMBRE 2026

Tema: Llamadas que cuestan libertad: El nuevo modelo de fraude telefónico en Venezuela

El nuevo modelo de fraude telefónico en Venezuela que simula privaciones de libertad combina técnicas psicológicas extremas, suplantación de identidad oficial y manipulación digital bajo la modalidad conocida como secuestro virtual.



El Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (Cicpc) y el Comando Nacional Antiextorsión y Secuestro (Conas) han emitido alertas urgentes ante el incremento de estas llamadas que provienen principalmente de centros carcelarios o de números con prefijos internacionales.

¿Cómo opera este modelo de fraude?

Los delincuentes ya no actúan al azar; utilizan bases de datos filtradas con información real de las víctimas (nombres completos, cédulas, datos de familiares y zonas de residencia) para que el engaño parezca legítimo.

1. Los estafadores contactan a un ciudadano simulando ser comisarios del Cicpc o miembros de grupos armados. Bajo falsas acusaciones de investigación criminal o amenazas directas, ejercen una presión psicológica tan alta que obligan a la persona a no colgar el teléfono.

2. Utilizan el pánico del momento, herramientas de Inteligencia Artificial para clonar voces o fotografías manipuladas digitalmente para exigir pagos urgentes en dólares a cambio de una supuesta liberación. Aunque la víctima nunca estuvo retenida físicamente, el secuestro se vuelve real para su familia a través de la desinformación.

3. Llaman asegurando que el teléfono de la víctima fue clonado o está vinculado a un delito. Solicitan que se les dicte un código que llegará por mensaje de texto para "limpiar" su nombre, el cual realmente es el código de verificación para apoderarse de la cuenta de WhatsApp.

4. Delincuentes se hacen pasar por agentes de soporte de Movistar, Digitel o Movilnet. Ofrecen supuestas migraciones gratuitas a redes 5G o bonos de saldo con el único fin de que la víctima les entregue credenciales o active el altavoz para vulnerar sus cuentas bancarias.

5. Configuran desvíos no autorizados en las líneas telefónicas mediante códigos rápidos, lo que les permite interceptar las llamadas del banco o de plataformas de mensajería para robar los códigos de seguridad.

Medidas de seguridad y qué hacer



- **Corte la comunicación de inmediato:** Si recibe una llamada de números extraños, con tono amenazante o de supuestos cuerpos policiales notificando delitos, cuelgue.

- **Verifique antes de actuar:** Si le aseguran que un familiar está retenido, intente contactar a esa persona por vías alternas o llame a su círculo cercano para comprobar dónde se encuentra antes de caer en pánico

- **Revise su línea:** Puede verificar si su teléfono tiene desvíos activos marcando el código *#21#. En caso de detectar un número desconocido asociado, marque ##002# para desactivar cualquier redirección oculta.

- **No entregue códigos:** Jamás comparta con terceros las claves que reciba por SMS o WhatsApp, ni siquiera si el interlocutor parece poseer sus datos personales de identidad.

La sofisticación de las estafas telefónicas y el uso de la ingeniería social en Venezuela demuestran que la legitimación de capitales ya no depende únicamente de complejas estructuras corporativas ficticias, sino de la manipulación inmediata de la identidad y de la banca de ciudadanos comunes

Fuente:

Agencia Venezolana de Noticias.
https://avn.info.ve/cicpc-detiene-a-tres-personas-por-estafa-mediante-aplicacion-de-credito-en-caracas/
Cuerpo de Investigaciones Científicas, Penales y Criminalísticas.
https://www.instagram.com/reel/Dd3taqHCEQl/
Bolsa de Valores de Caracas.
https://www.bolsadecaracas.com/