LUN

Fecha: 25/08/2025 Audiencia: 271.020 Sección: NACIONAL
Vpe: $3.947.205 Tirada: 91.144 Frecuencia: DIARIO
Vpe pág: $4.399.200 Difusión: 91.144
Vpe portada: $4.399.200 Ocupación: 89,73%

Darío Betti, director del Mobile Ecosystem Forum, advierte sobre las nuevas tácticas de fraudes digitales

"En el primer semestre de 2025 WhatsApp desactivó 6,8 millones de cuentas vinculadas a centros de estafa"

"En la cima hay redes transnacionales muy estructuradas, que funcionan como empresas, que contratan, capacitan y hasta explotan a personas obligadas a estafar", plantea.

IGNACIO MOLINA (LONDRES)

En el edificio Spaces, junto a la estación de Metro y Tren de Finsbury Park, tiene su sede el Mobile Ecosystem Forum, una organización internacional que agrupa a empresas de telecomunicaciones y servicios digitales en más de 40 países. Fundado en el 2000, celebra 25 años como referente en la lucha contra el fraude digital y en la creación de estándares de seguridad.

Desde esa oficina, su director ejecutivo, Darío Betti, dice: "Chile enfrenta la misma ola de estafas digitales híbridas que vemos en el mundo. Ya no se parecen al phishing clásico (combina SMS, WhatsApp, cuentas falsas en redes sociales e incluso voces clonadas de call centers, de modo que la estafa parece oficial)". Betti dirige el MEF desde 2019. Participó en T-Mobile en el lanzamiento del primer servicio de internet móvil en Europa y hoy lidera un gremio que busca anticiparse a las estafas tecnológicas y coordinar defensas conjuntas.

"En Chile hemos visto un fuerte aumento del smishing (una forma de phishing o fraude digital en que se envían SMS falsos para robar claves y datos) en los últimos dos años. Las estafas más comunes reportadas son las que suplantan a bancos. Esto incluye mensajes falsos de BancoEstado, Banco de Chile, Santander, etcétera, normalmente, alertando de fraudes o cuentas bloqueadas. El enlace lleva a un clon de la web del banco que roba datos y contraseñas. Los delincuentes también aplican la misma técnica con mensajes de reparto, correos, DHL y organismos públicos o de servicios, por ejemplo, el Servicio de Impuestos Internos", detalla Betti, máster en Gestión de Medios por la University of Stirling.

El diagnóstico es claro: las estafas digitales ya no buscan un descuido, sino construir confianza con varios pasos encadenados.

IGNACIO MOLINA

"Usan países con regulación débil o fragmentada", dice Betti.

"Las trampas más sofisticadas suplantan instituciones legítimas en varias capas: un SMS que lleva a un chat en WhatsApp y luego a una llamada con una voz generada por Inteligencia Artificial. La gente en Chile debe entender que esa 'confianza' se construye artificialmente a través de una cadena de canales. WhatsApp tiene una penetración del 80% en Chile y hemos visto un aumento de fraudes en esa vía también", comenta Betti.

¿Quiénes están detrás de estas estafas?

"El smishing y el fraude por SMS ya no son obra de individuos aislados. Aunque un operador solitario pueda lanzar campañas pequeñas, la mayoría proviene de grupos organizados o redes criminales internacionales. En la base están proveedores de 'fraude como servicio', que venden kits de phishing o acceso a SIM comprometidas. Luego hay grupos medianos especializados en un tipo de fraude, que operan con call centers o plataformas automatizadas. En la cima hay redes transnacionales muy estructuradas, que funcionan como empresas, que contratan, capacitan y hasta explotan a personas obligadas a estafar".

¿Dónde se ubican y por qué son difíciles de rastrear?

"Son operaciones profesionales, con programadores, operadores de call center y gerentes financieros. Se distribuyen como nómadas digitales, en países con baja fiscalización. No son improvisados: eligen lugares estratégicos donde la aplicación de la ley es débil".

¿Cómo mueven el dinero?

"Usan países con regulación débil o fragmentada: África Occidental, Europa del Este, partes de Latinoamérica y cada vez más el Sudeste Asiático. Se ocultan con números virtuales, apps encriptadas y servidores que cambian constantemente. También hemos visto ejemplos en Reino Unido, con cuentas bancarias falsas locales. El sector financiero todavía tiene mucho que mejorar en velocidad de respuesta y defensas internas".

¿Qué dato internacional refleja la magnitud de este problema y su proyección en Chile?

"En el Reino Unido, el año pasado, el fraude por suplantación representó casi el 40% de las estafas reportadas, con pérdidas superiores a 1.200 millones de libras. Canales como SMS y mensajería OTT -WhatsApp, iMessage- fueron claves. En el primer semestre de 2025 WhatsApp desactivó 6,8 millones de cuentas vinculadas a centros de estafa, muchos en el Sudeste Asiático. Eran fraudes de criptomonedas, empleos falsos, promesas de dinero por tareas simples como dar like en TikTok. No hay razón para pensar que Chile será distinto en el futuro".

¿Cuáles estrategias han demostrado reducir estos fraudes?

"En Reino Unido creamos registros compartidos para bloquear remitentes falsos a nivel de red. En Nigeria, fuerzas de tarea público privadas filtran tráfico sospechoso antes de llegar al usuario. La clave está en que telecomunicaciones, bancos y reguladores compartan inteligencia en tiempo real y se alíneen en estándares técnicos. Educar no basta, hay que modificar hábitos. El social engineering (engaño digital basado en manipular la confianza y las emociones de las personas) funciona porque altera reacciones instintivas. Un ejemplo: Apple, en (el sistema operativo) iOS 26 separa los SMS de números desconocidos en otra bandeja. Es un filtro automático, sin necesidad de educación. Pero generó resistencia, la gente depende de mensajes únicos de bancos, hospitales o repartos, y muchos no encuentran esos SMS".

¿Qué consejos daría a los usuarios en Chile para no caer en estas estafas?

"La clave es pausar antes de actuar. Los estafadores dependen de crear urgencia. Decir 'llamaré mañana' o usar un canal verificado casi siempre rompe la estafa. Puede sonar extraño, pero si recibe un mensaje sobre una supuesta emergencia, no reaccione. Espere unos minutos, siéntese, respire. Luego piense cómo suele contactar a esa empresa: ¿con un número guardado?, ¿con la app oficial? No responda directamente al mensaje".