LUN

Fecha: 26/05/2026 Audiencia: 271.020 Sección: ACTUALIDAD
Vpe: $2.288.464 Tirada: 91.144 Frecuencia: 0
Vpe pág: $4.399.200 Difusión: 91.144
Vpe portada: $4.399.200 Ocupación: 52,02%

El nuevo fraude aprovecha una antigua función de desvío de llamadas disponible en la mayoría de los celulares

El código que jamás hay que marcar si lo llaman "del banco": así funciona la estafa del *21

Especialistas advierten que el fraude no hackea el teléfono, pero sí permite interceptar SMS y llamadas usados para recuperar claves, validar accesos o tomar control de cuentas digitales.

Banco de Chile alertó a sus clientes.

DANIELA TORÁN

"Detectamos movimientos sospechosos en su cuenta". "Intentaron hackear su banco". "Necesitamos proteger sus datos ahora". Con frases como esas comienza la nueva modalidad de estafa telefónica que motivó una alerta enviada por Banco de Chile a sus clientes.

El fraude utiliza el código *21, una función real y antigua de los celulares que permite desviar llamadas hacia otro número telefónico. El problema es que los delincuentes convencen a las víctimas de activarlo sin saber lo que realmente están haciendo.

La técnica corresponde a un tipo de vishing, es decir, phishing mediante llamadas telefónicas. Los delincuentes se hacen pasar por ejecutivos bancarios, personal de seguridad, soporte técnico o incluso policías. Siempre apelan a la urgencia.

Muy simple

El subcomisario de la Brigada Investigadora del Cibercrimen de la PDI, Esteban Donoso, explica que el mecanismo es más simple de lo que parece.

"Los delincuentes solicitan que las personas coloquen el asterisco 21 junto con un número telefónico que ellos mismos entregan. Cuando la víctima realiza esa acción, las llamadas telefónicas y los mensajes de texto pasan a reenviarse a ese otro número", señala.

Donoso aclara que no se trata de un hackeo del teléfono. "La víctima no pierde el control de su dispositivo ni de sus aplicaciones. Lo que pierde es el control de la información que llega al teléfono, porque las llamadas y en varios casos los SMS son redirigidos al número del delincuente", detalla.

Ahí aparece el verdadero riesgo. Muchas plataformas todavía utilizan mensajes SMS o llamadas para recuperar contraseñas o validar accesos.

"Si los delincuentes logran bloquear una cuenta bancaria con el rut y claves erróneas, y después solicitan una recuperación de clave vía SMS, ese mensaje ya no le llega al usuario real. Le llega directamente al número que ellos configuraron mediante el desvío", advierte el detective.

Y para qué

Una vez dentro de la cuenta, agrega, los estafadores pueden cambiar claves y acceder a distintos productos bancarios. "Muchas veces no necesitan transferir dinero directamente. Lo que hacen es pedir avances, solicitar créditos o utilizar tarjetas de crédito, porque para eso basta con acceder a los datos completos de la tarjeta. Para las transferencias es más difícil porque hay entidades que usan otro código de autentificación, como claves en aplicaciones, tarjetas de coordenadas o lectura biométrica", dice.

No solo el banco

El ingeniero industrial y experto en sistemas de la Universidad de Santiago (Usach), Diego Fuentealba, recalca que el peligro no se limita a las cuentas bancarias.

"WhatsApp, Google, Apple y otras plataformas también utilizan SMS o llamadas como método de recuperación de cuentas. Entonces, si el delincuente recibe esos códigos, eventualmente podría tomar control del WhatsApp o del correo electrónico de una persona", afirma.

Eso puede derivar en nuevas estafas. "Si controlan el WhatsApp, después pueden escribirles a familiares o amigos haciéndose pasar por la víctima y pedir dinero. Ahí ya entramos en otro tipo de fraude", agrega.

Fuentealba enfatiza que el código *21 no es algo malicioso por sí mismo. "Los teléfonos celulares tienen desvío de llamadas hace muchísimos años. Lo que están haciendo los delincuentes es aprovechar una función normal del teléfono y el desconocimiento de las personas", explica.

También advierte que el impacto depende de cómo tenga configuradas sus cuentas cada usuario. "Hay bancos y aplicaciones que utilizan sistemas más robustos, como biometría o aplicaciones de autenticación. Pero todavía existen plataformas que usan SMS como método de recuperación o validación", sostiene.

Banco de Chile advirtió a sus clientes que nunca solicitará marcar códigos por teléfono ni entregar claves o datos personales durante llamadas.

Mejor cortar

Entre las principales señales de alerta están las llamadas desde números desconocidos, supuestos ejecutivos bancarios, escenarios de urgencia y solicitudes para marcar códigos o compartir información sensible.

Los expertos recomiendan cortar inmediatamente la llamada y contactar al banco solo a través de canales oficiales.

Para revisar si existe un desvío activo en el teléfono, se puede marcar *#21#. Y si aparece una redirección desconocida, el desvío puede eliminarse digitando ##21#.