LITORALPRESS

Fecha: 20-05-2026
Medio: El Insular
Supl. : El Insular
Tipo: Noticia general
Título: Nueva estafa telefónica en Chile: así funciona el fraude que utiliza el código *21 para acceder a datos bancarios

Pág. : 13
Cm2: 563,0

Tiraje: 2.500
Lectoría: 7.500
Favorabilidad: No Definida

Nueva estafa telefónica en Chile: así funciona el fraude que utiliza el código *21 para acceder a datos bancarios

Especialista advierte que las nuevas modalidades de vishing combinan filtración de datos, manipulación psicológica y herramientas de IA para vulnerar incluso a usuarios con experiencia digital y acceso frecuente a banca online.

Diversas entidades financieras han alertado durante los últimos días sobre una nueva modalidad de fraude telefónico conocida como **"vishing"**, una técnica de ingeniería social que busca engañar a las personas mediante llamadas falsas para obtener acceso a información sensible y cuentas bancarias.

La estafa consiste en llamadas realizadas por delincuentes que se hacen pasar por ejecutivos bancarios o representantes de instituciones conocidas. Bajo un escenario de urgencia, advierten sobre supuestos movimientos sospechosos o problemas de seguridad y solicitan a la víctima marcar códigos como ***21** desde su teléfono, acción que permite desviar llamadas y eventualmente interceptar códigos de verificación y autorizaciones bancarias.

Según explicó Diego Cáceres, académico de la Escuela de Tecnología de la Universidad UNIACC, ***"el vishing ha evolucionado desde llamadas masivas y poco creíbles a operaciones altamente sofisticadas de ingeniería social. Hoy los atacantes utilizan filtraciones de datos, spoofing telefónico para aparentar números legítimos, inteligencia artificial para clonar voces y campañas coordinadas por WhatsApp, SMS y llamadas".***

El especialista sostuvo que el fenómeno ha aumentado en Chile debido a la expansión de la digitalización financiera y al uso del teléfono móvil como eje central de autenticación bancaria.

"Las bandas criminales entendieron que es más rentable engañar personas que vulnerar infraestructura técnica. Además, las cifras de fraudes financieros y reclamos han aumentado de forma importante en los últimos años, lo que demuestra que el problema ya es masivo y no aislado", afirmó.

A juicio del docente, uno de los elementos más complejos de este tipo de fraude es que logra afectar incluso a usuarios con conocimientos tecnológicos o experiencia digital. ***"El vishing no apunta solamente a explotar una debilidad técnica, sino una reacción humana. Incluso personas con conocimientos en ciberseguridad pueden caer cuando el atacante mezcla urgencia, presión emocional y contexto real"***, indicó.

"Hoy los delincuentes llegan con información filtrada: nombre, banco, últimas compras o incluso datos familiares. Eso hace que la llamada parezca legítima. Además, cuando se activa el estrés, por ejemplo, con frases como 'están vaciando su cuenta ahora', el cerebro prioriza reaccionar rápido antes que verificar. La ingeniería social moderna está diseñada precisamente para saltarse el pensamiento racional. Y con IA generativa y clonación de voz, el nivel de realismo es muchísimo mayor que hace algunos años".

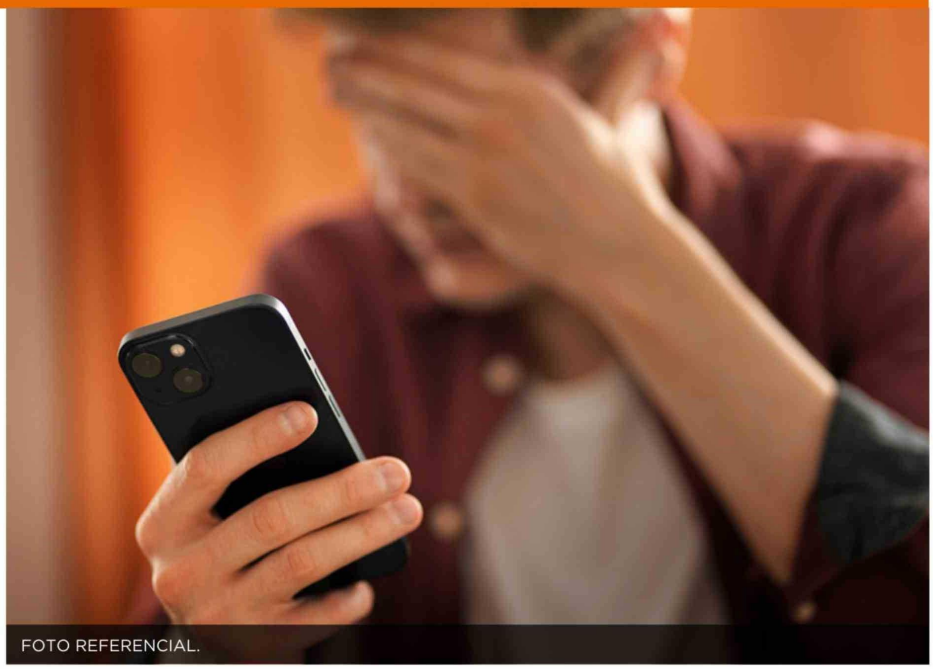

FOTO REFERENCIAL.

Respecto de los usuarios más afectados, explicó que tradicionalmente los adultos mayores eran el principal objetivo de estas estafas, aunque hoy el panorama cambió. ***"Las bandas también están apuntando a jóvenes digitalizados, profesionales y personas con acceso frecuente a banca online. De hecho, quienes más confían en sus conocimientos tecnológicos muchas veces subestiman el riesgo"***, sostuvo.

Asimismo, advirtió que también son vulnerables las personas bajo altos niveles de estrés, trabajadores que manejan múltiples cuentas o usuarios que realizan operaciones rápidas desde el celular durante la jornada laboral.

Cáceres enfatizó que las campañas de prevención no siempre logran el mismo ritmo de adaptación que las nuevas modalidades de fraude. ***"Las tácticas cambian más rápido que la educación del usuario promedio. Además, existe fatiga digital: la gente ya está saturada de alertas, notificaciones y advertencias. Eso provoca que muchos bajen la guardia"***, advirtió.

Frente a este escenario, el especialista en ciberseguridad recomendó no entregar claves, códigos SMS, tokens ni aprobar operaciones durante llamadas telefónicas. Además, aconsejó activar autenticación multifactor, mantener bloqueado el teléfono y proteger aplicaciones críticas —como las bancarias— con biometría o claves distintas a las del dispositivo, verificando siempre cualquier contacto mediante canales oficiales.

"Ningún banco serio debería pedir claves o códigos durante una llamada. Hoy también es importante revisar las configuraciones del teléfono, porque algunas campañas están usando desvío de llamadas mediante códigos para interceptar verificaciones bancarias", explicó.

El experto también llamó a cortar inmediatamente cualquier comunicación sospechosa y evitar actuar bajo presión emocional. ***"Se recomienda revisar movimientos recientes, cambiar contraseñas si alcanzó a entregar algún dato y reportar el incidente. En ciberseguridad, desconfiar a tiempo vale más que reaccionar tarde. Muchas veces el fraude se evita simplemente rompiendo el flujo emocional que el atacante intenta controlar"***, concluyó.