LITORALPRESS

Fecha: 31-01-2026
Medio: Diario El Cóndor
Supl. : DIARIO EL CONDOR
Tipo: Noticia general
Título: Alerta por estafas digitales que usan emergencias para robar cuentas de WhatsApp

Pág. : 4
Cm2: 214,8
VPE: $ 26.854

Tiraje: 500
Lectoría: 1.500
Favorabilidad: No Definida

Alerta por estafas digitales que usan emergencias para robar cuentas de WhatsApp

En medio de la emergencia provocada por los incendios forestales que aún afectan al sur del país, las autoridades han encendido las alarmas ante una modalidad de estafa digital que se vale de la suplantación de identidad de instituciones públicas —como Carabineros o la Fiscalía Nacional— para embaucar a víctimas y familiares de personas afectadas, con el objetivo de tomar control de sus cuentas de WhatsApp y perpetrar fraudes posteriores.

Este tipo de engaños se inserta en un escenario de fuerte aumento de los delitos asociados al fraude en el país. Según datos oficiales del Poder Judicial, al cierre del tercer trimestre de 2025 se registraron 41.703 causas penales por fraude, la cifra más alta desde que se comenzaron a llevar registros en 2013, evidenciando un crecimiento sostenido del fenómeno, especialmente vinculado a estafas y defraudaciones.

En algunos de los casos denunciados ante las autoridades, los estafadores contactaron a familiares de víctimas de incendios en comunas como Penco y Tomé, simulando ser funcionarios policiales con supuesta "información reservada". Bajo ese pretexto, instan a las personas a ingresar a enlaces maliciosos o a entregar códigos de verificación enviados por WhatsApp, lo que permite a terceros acceder a la cuenta y, posteriormente, solicitar dinero o realizar otros fraudes en nombre de la víctima.

Este patrón no es aislado. A nivel institucional, en noviembre de 2025 la Comisión para el Mercado Financiero (CMF) emitió una alerta pública advirtiendo sobre estafas que suplantaban su identidad y la de sus funcionarios mediante llamadas telefónicas, documentación falsa y correos electrónicos, reforzando la preocupación por el uso de identidades oficiales para generar confianza y concretar engaños.

Frente a este escenario, Nicolás Silva, director de Tecnología de Asimov Consultores, explica que este tipo de ataques se basa en técnicas de ingeniería social y en la explotación de la urgencia emocional de las personas afectadas. "Ninguna institución legítima solicita que ingreses a un enlace ni que entregues códigos por WhatsApp, mensaje de texto o llamada para informar sobre un familiar o una situación personal. Esa es una señal clara de fraude", advierte.

El especialista agrega que los códigos de verificación son "la llave de acceso a las cuentas", y que compartirlos con terceros facilita la suplantación de identidad y la extensión del fraude hacia los contactos de la víctima. Por ello, enfatiza que "ante cualquier contacto inesperado, lo adecuado es no abrir enlaces, no compartir códigos ni entregar información personal, incluso si el mensaje parece provenir de una institución oficial".

En Chile y en la región, los fraudes digitales se han vuelto más frecuentes, especialmente aquellos en los que los estafadores imitan comunicaciones legítimas para solicitar información o generar acciones rápidas. Esto hace que la educación digital sea un pilar fundamental para que las personas puedan identificar señales tempranas y proteger su información.

Desde Asimov Consultores, la recomendación es "verificar siempre la identidad de quien realiza el contacto a través de canales oficiales, evitar abrir enlaces no solicitados y desconfiar de solicitudes de dinero o datos, incluso cuando provengan de contactos conocidos, especialmente en situaciones de emergencia". En un escenario marcado por un aumento histórico de las causas penales por fraude en Chile, el llamado es "a reforzar la educación y las buenas prácticas de seguridad digital, ya que la creciente sofisticación de los engaños exige mayores niveles de prevención tanto a nivel individual como organizacional".