LITORALPRESS

Fecha: 18-01-2026
Medio: La Tercera
Supl. : La Tercera - Edición Especial II
Tipo: Noticia general
Título: **Los tres fraudes digitales más frecuentes en el país**

Pág. : 2
Cm2: 716,1

Tiraje: 78.224
Lectoría: 253.149
Favorabilidad: No Definida

[ CIBERSEGURIDAD ]

# Los tres fraudes digitales más frecuentes en el país

**Aunque se tratan de engaños a través de plataformas distintas, los tres buscan el mismo objetivo: que los usuarios entreguen sus claves.**

**Por: Sofía Cruces**

**El avance de las herramientas digitales** ha sido beneficioso para todos, sin embargo, se vuelve problemático cuando algunos crimininales las utilizan para atacar a otros.

Y entre los delitos más comunes se encuentran el phishing, el vishing y el smishing. Según Francisco Fernández, gerente general de AVANTIC CHILE, empresa de servicios y soluciones de ciberseguridad, se trata de las tres estafas digitales más frecuentes en el país.

El phising se refiere a correos electrónicos falsos, mientras que el vishing corresponde a llamadas telefónicas engañosas y el smishing a mensajes de texto con enlaces sospechosos.

"De esta forma los delincuentes buscan inducir a las víctimas a revelar datos sensibles, tales como claves de acceso, información bancaria o códigos de verificación", explicó Fernández.

Según el experto, los mensajes utilizados suelen estar minuciosamente elaborados con el fin de generar alarma o confianza, apelando a situaciones como bloqueos de cuentas, supuestas irregularidades, beneficios exclusivos o premios inexistentes.

Sin embargo, cuando el usuario responde a estas solicitudes o accede a enlaces maliciosos, queda expuesto a robos de dinero, usurpación de identidad y otros delitos asociados.

## Medidas de protección

Frente al hecho de que las herramientas con las que se está perjudicando a personas no se van a ir y tampoco hay certezas sobre si se lograrán regular, el experto en ciberseguridad de AVANTIC CHILE entrega se recomendaciones para dismunuir los riesgos:

**1. Construir contraseñas fuertes y únicas** para cada plataforma, e implementar doble factor de autenticación para aplicaciones como WhatsApp, correo electrónico, y demás aplicaciones que pudieran contener información sensible del usuario.

**2. Mantener actualizados los dispositivos y las aplicaciones,** asegurando que cuenten con las últimas medidas de seguridad y protección.

**3. No revelar nunca contraseñas, códigos de seguridad ni datos bancarios** por medio de correos electrónicos, llamadas telefónicas o aplicaciones de mensajería.

**4. Adoptar una postura de desconfianza ante mensajes inesperados** que soliciten información personal o financiera.

**5. No acceder a enlaces ni descargar archivos adjuntos** que provengan de remitentes desconocidos o no verificados.

**6. Dado que la IA permite crear mensajes extremadamente personalizados y aparentemente legítimos, resulta fundamental chequear la veracidad de cualquier solicitud** contactando directamente a la institución correspondiente mediante sus canales oficiales de comunicación.

Finalmente, Fernández sugiere que a las personas reporten cualquier intento de estafa a las instituciones afectadas y a las autoridades correspondientes, como una manera de contribuir a potenciar las acciones de prevención y persecución de este tipo de delitos.

"Fomentar una cultura de seguridad digital y fortalecer el conocimiento sobre estas ciberamenazas es crucial para disminuir sus efectos", concluyó el gerente general de AVANTIC CHILE.

> "Los delincuentes buscan inducir a las víctimas a revelar datos sensibles, tales como claves de acceso, información bancaria o códigos de verificación".
>
> **FRANCISCO FERNÁNDEZ,** AVANTIC CHILE