

Dan consejos para prevenir las estafas bancarias y qué hacer ante un fraude

DELITOS. Casos recientes de alto impacto, como el que afectó a la actriz Amparo Noguera, evidencian el avance de los delitos financieros. La banca y especialistas advierten sobre nuevas modalidades de engaño.

Karen Elena Cereceda Ramos
 karen.cereceda@mercuriocalama.cl

A TENER EN CUENTA

Estar alertas:

- Llamadas que exigen acciones urgentes.
- Mensajes con enlaces o códigos QR inesperados.
- Solicitud de claves, códigos o datos personales.
- Ofertas o premios demasiado convenientes.

Consejos:

- No perder de vista la tarjeta al pagar.
- Revisar cajeros automáticos antes de operar.
- Cortar llamadas sospechosas y contactar directamente a su banco.
- Bloquear productos si le roban o extravía el celular.

Emergencia:

- Bloquear de inmediato los medios de pago.
- Cambiar contraseñas.
- Llamar al 1212.
- Denuncia ante banco, PDI, Fiscalía y/o Sernac.

un computador.

“Yo siempre decía que la gente caía porque no se informaba, yaun así caí. Estas personas son muy convincentes y manejan información que uno cree privada, como números de tarjetas o movimientos”, señaló.

El testimonio da cuenta de que los delincuentes utilizan un lenguaje técnico y estrategias de presión que generan temor y sensación de urgencia. “No sólo atacan a quienes tienen cuentas corrientes o grandes montos



DELINCUENTES BUSCAN OBTENER INFORMACIÓN PERSONAL Y FINANCIERA PARA ACCEDER A CUENTAS BANCARIAS Y SUSTRAYER DINERO.

1212 es el número telefónico

que agrupa a todos los bancos de Chile, donde se puede comunicar el cliente.

de dinero, sino a todas las personas, sin distinción”, agrega.

Tras darse cuenta del engaño, la víctima realizó la denuncia tanto en su banco como ante la Fiscalía, sin que hasta ahora haya recibido una respuesta o resolución a su caso.

PREVENCIÓN Y RIESGOS

En este contexto, la ABIF mantiene activa la campaña #OSPeche, orientada a informar sobre los principales tipos de fraude, como el phishing, smishing, vishing, estafas por redes sociales, códigos QR maliciosos, programas maliciosos y clonación de tarjetas. La iniciativa busca que las personas identifiquen señales de alerta y eviten compartir datos sensibles.

Como parte de estas acciones, la banca implementó el número de emergencias bancarias

“Es clave que las personas adopten medidas preventivas, se informen y, en caso de emergencia, contacten de inmediato a su banco llamando al 1212”.

Luis Opazo
 Gerente Gral. de ABIF

1212, gratuito y disponible a nivel nacional, que deriva directamente a las plataformas de atención de cada banco.

Desde su lanzamiento, hace un mes, cerca de 35 mil personas han utilizado este servicio, con un tiempo promedio de respuesta de 22 segundos. “Es clave que las personas adopten medidas preventivas, se informen y, en caso de emergencia, contacten de inmediato a su banco llamando al 1212 ante cualquier situación sospechosa”, señaló Luis Opazo, gerente general de la ABIF.

Sobre los riesgos, los especialistas advierten que los riesgos aumentan durante el período

“Es importante evitar enlaces sospechosos, desconfiar de descuentos demasiado atractivos y verificar siempre que el sitio sea legítimo”.

Maite Aguirrezaibá
 Abogada UANDES

do de vacaciones, cuando se incrementa el uso de dispositivos móviles, redes Wi-Fi públicas y compras online.

La directora del Departamento de Derecho Procesal y Litigación de la Universidad de los Andes, Maite Aguirrezaibá, señala que en estas fechas se intensifican prácticas como sitios web clonados, ofertas falsas en redes sociales, carding, códigos QR maliciosos y aplicaciones fraudulentas.

“Es importante evitar enlaces sospechosos, desconfiar de descuentos demasiado atractivos y verificar siempre que el sitio sea legítimo”, explica la académica de la Universidad.

Ante cualquier indicio de fraude, añade, se deben bloquear los medios de pago, cambiar contraseñas y denunciar ante el banco, la PDI y el Sernac, lo que permite activar mecanismos de protección y seguimiento.

Desde la industria de la ciberseguridad advierten que una parte importante de los incidentes tiene un componente humano, situación que se acentúa durante los períodos de descanso.

En el ámbito doméstico, el uso de redes Wi-Fi públicas y dispositivos personales incrementa la exposición a fraudes, mientras que en las organizaciones la gestión informal de accesos y credenciales eleva los riesgos de uso no autorizado.

La recomendación, coinciden expertos y autoridades, es mantener hábitos digitales responsables, desconfiar de contactos inesperados y actuar con rapidez ante cualquier señal de alerta, ya que la prevención sigue siendo la principal herramienta para evitar pérdidas económicas de alto impacto.