

### ¿Qué es PHISHING?

- E-mail fraudulento diseñado para robar datos de usuarios de bancos u otras empresas conocidas.
- Los usuarios poco informados son engañados para que entreguen contraseñas, números de tarjetas de crédito, carné de identidad u otros.

### ¿Cómo reconocer PHISHING?

- **Solicitan información personal.** Ninguna empresa debe pedir que envíes tu contraseña, nombre de usuario o cualquier otro dato personal por correo electrónico.
- **No son personalizados.** Los mensajes de "phishing" suelen enviarse de forma masiva y **no contienen tu nombre o apellido**. El Banco de Chile se dirige a ti con nombre y apellido.
- **Anuncian cierre de cuenta** "En un plazo de 48 horas, tu cuenta quedará cerrada." El tono de los mensajes de "phishing" están diseñados para provocar una sensación de urgencia y responder sin pensar.
- **Solicitan hacer clic para acceder a tu cuenta.** Los mensajes de "phishing" tienen un link o formulario para completar tal como lo haría un sitio web. Aunque no entregues datos personales, puedes estar descargando un virus que registra la actividad del teclado. Los correos del Banco de Chile **jamás tienen link directo al login**. Sólo pueden derivar a una revista digital, como En Línea Digital o Travel News Digital, donde **jamás se solicita clave o datos personales**.
- **Errores de ortografía o tipográficos.** Los mensajes de "phishing" suelen estar mal redactados o con falta de ortografía, debido a que suelen ser de origen extranjero.

### Consejos para evitar el PHISHING :

- Sé cuidadoso al hacer clic en vínculos incluidos en el e-mail. Banco de Chile, **no envía, no ha enviado ni enviará** a sus clientes e-mails solicitando ingresar datos personales como clave secreta o números de cuentas.
- Siempre ingresa a los sitios del Banco de Chile digitando directamente en la barra de dirección del explorador [www.bancochile.cl](http://www.bancochile.cl), donde podrás operar con total confianza.
- No introduces información personal ni financiera en ventanas que emerjan de un e-mail.
- Utiliza DigiPass – Llave Electrónica de Alta Seguridad, que impide que terceros operen en tu cuenta, incluso si contaran con tu clave de acceso a Banco en Línea. Si no lo tienes, solicítalo ahora en [bancochile.cl](http://bancochile.cl) o en (600)-637-3000.
- Comprueba periódicamente los estados de tu cuenta corriente y tarjetas de crédito.

### Qué hacer si fuiste víctima de PHISHING

- En caso que hayas hecho clic o que hayas entregado información personal en un e-mail sospechoso, sigue inmediatamente los siguientes pasos:
  - Paso 1: Cambia inmediatamente las contraseñas de todas tus cuentas
  - Paso 2: Ante una comunicación electrónica sospechosa a nombre del Banco de Chile, ingresa a nuestro sitio verificando que no exista una advertencia al respecto. Infórmanos del incidente escribiéndonos a Contacto en [bancochile.cl](http://bancochile.cl) o llámanos a la Mesa de Ayuda Internet (600) 637 3000.
  - Paso 3: Ejecuta inmediatamente software antivirus y antiespía actualizado. Puedes descargalo [desde aquí](#).