



CIBERCONSEJOS PARA IDENTIFICAR UN PHISHING



¿QUÉ ES UN PHISHING?

Técnica que busca engañar a las víctimas, haciéndose pasar por una persona, empresa o servicio de confianza. Se realiza por correo electrónico, SMS o apps de mensajería, en los que los delincuentes presionan a las personas a ingresar a un link con el objetivo de dirigirlos a una web fraudulenta y así robar su información.



CARACTERÍSTICAS DEL PHISHING

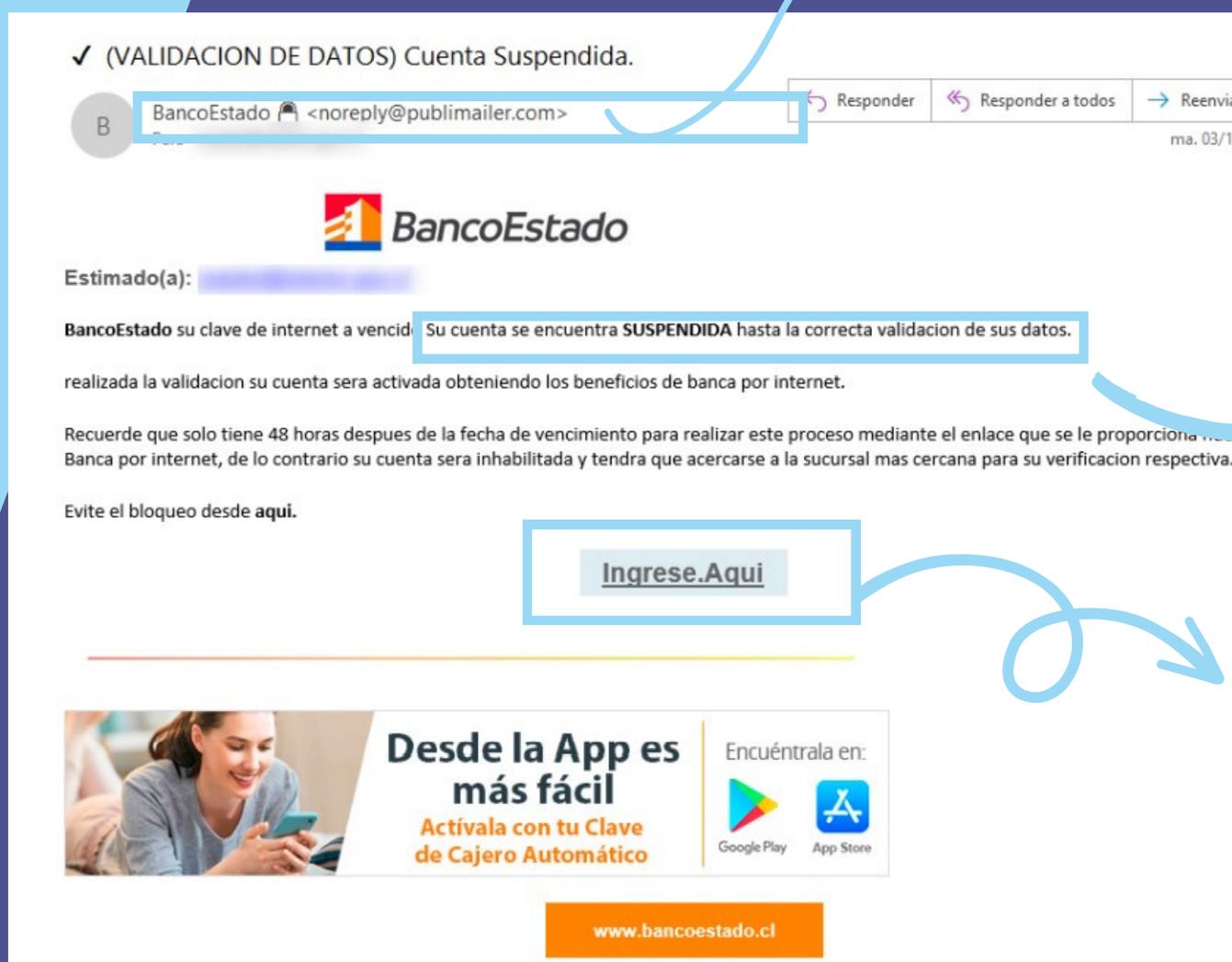
- ✉ Incluye contenido alarmante o urgente.
- ✉ Asusta con bloques de tarjetas o cuentas bancarias.
- ✉ Tiene faltas de ortografía o imágenes de mala calidad.
- ✉ Solicita contraseñas, información personal o realizar un pago.
- ✉ Adjunta documentos o facturas que no fueron solicitados.
- ✉ El remitente es desconocido y no proviene de la empresa aludida.



RECOMENDACIONES

Desconfiar si provienen de fuentes desconocidas.

Desconfía si el mensaje es alarmante.



✓ (VALIDACION DE DATOS) Cuenta Suspendida.

BancoEstado <noreply@publemailer.com>

ma. 03/10

BancoEstado

Estimado(a):

BancoEstado su clave de internet a vencido. Su cuenta se encuentra **SUSPENDIDA** hasta la correcta validacion de sus datos.

realizada la validacion su cuenta sera activada obteniendo los beneficios de banca por internet.

Recuerde que solo tiene 48 horas despues de la fecha de vencimiento para realizar este proceso mediante el enlace que se le proporciona en el correo. Si no realiza la validacion de su cuenta en el tiempo establecido, su cuenta sera inhabilitada y tendra que acercarse a la sucursal mas cercana para su verificacion respectiva.

Evite el bloqueo desde [aqui](#).

[Ingresa.Aqui](#)

Desde la App es más fácil
Activala con tu Clave de Cajero Automático

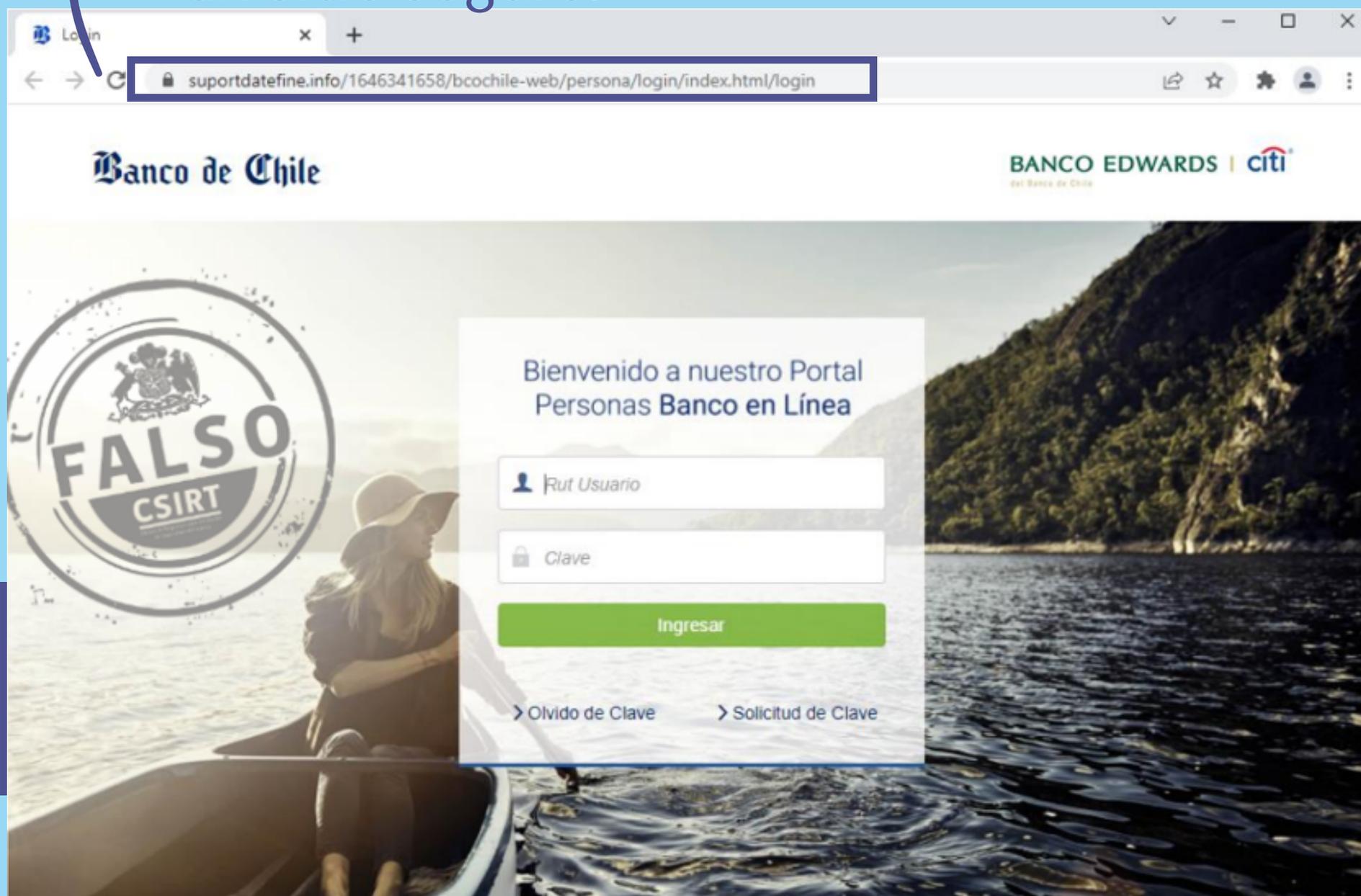
Encuéntrela en:
Google Play App Store

www.bancoestado.cl

Sospecha de links y archivos.

RECOMENDACIONES

Siempre revisa que la URL sea la correcta y recuerda: un candado no significa que sea un sitio seguro.





CIBERCONSEJOS

¿CÓMO ACTUAR EN CASO DE SER VÍCTIMA DE PHISHING?

1

ACTÚA RÁPIDO Y CAMBIA TU CONTRASEÑA

Comienza por aquellas cuentas que crees pueden estar comprometidas y en los sitios donde usas la misma clave.



REVISA TUS CUENTAS BANCARIAS

2

Verifica si tus tarjetas de crédito u otras cuentas tienen transacciones no reconocidas o autorizadas por ti.

En caso de tener movimientos desconocidos, contacta inmediatamente a tu institución financiera.



3

UTILIZA ANTIVIRUS O ANTIMALWARE

Este tipo de programas te permitirá buscar, detectar, eliminar y evitar una posible infección de malware (software malicioso) en tu computador.



INFORMA A TUS CONOCIDOS

4

Adviértele a tus contactos sobre el phishing para que estén atentos y no caigan en la misma trampa.



5

¡RECUERDA!

El phishing es una estafa que busca engañar a las víctimas, haciéndose pasar por una persona, empresa o servicio de confianza, a través de mensajes por correo electrónico, SMS o apps de mensajería, en los que los delincuentes presionan a las personas a ingresar a un link para dirigirlos a una web fraudulenta y así robar su información.

