

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



Alerta de seguridad cibernética	8FPH23-00892-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de septiembre de 2023
Última revisión	20 de septiembre de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER [ACÁ](#)

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing vía correo electrónico. En esta campaña, los delincuentes indican falsamente a la víctima lo siguiente:

*“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.”*

El correo electrónico incluye un enlace a un formulario para capturar credenciales de usuarios.

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 [@csirtgob](https://twitter.com/csirtgob)
 <https://www.linkedin.com/company/csirt-gob>

Indicadores de compromiso

Antes de evaluar la aplicación de acciones, tenga presente las advertencias de **gestión de los IoC**. Los IoC de este informe pueden ser obtenidos directamente desde nuestro **repositorio**.

URL del sitio falso

http://prevemed[.]com.ar/1695241888/imagenes/_personas/home/default.asp

URL de redirección

https://promezclas.com/activacion/cuenta-wckh/

IP del sitio falso

107.180.26.179

Asuntos del correo electrónico

Aviso Cuenta Temporalmente Suspendida

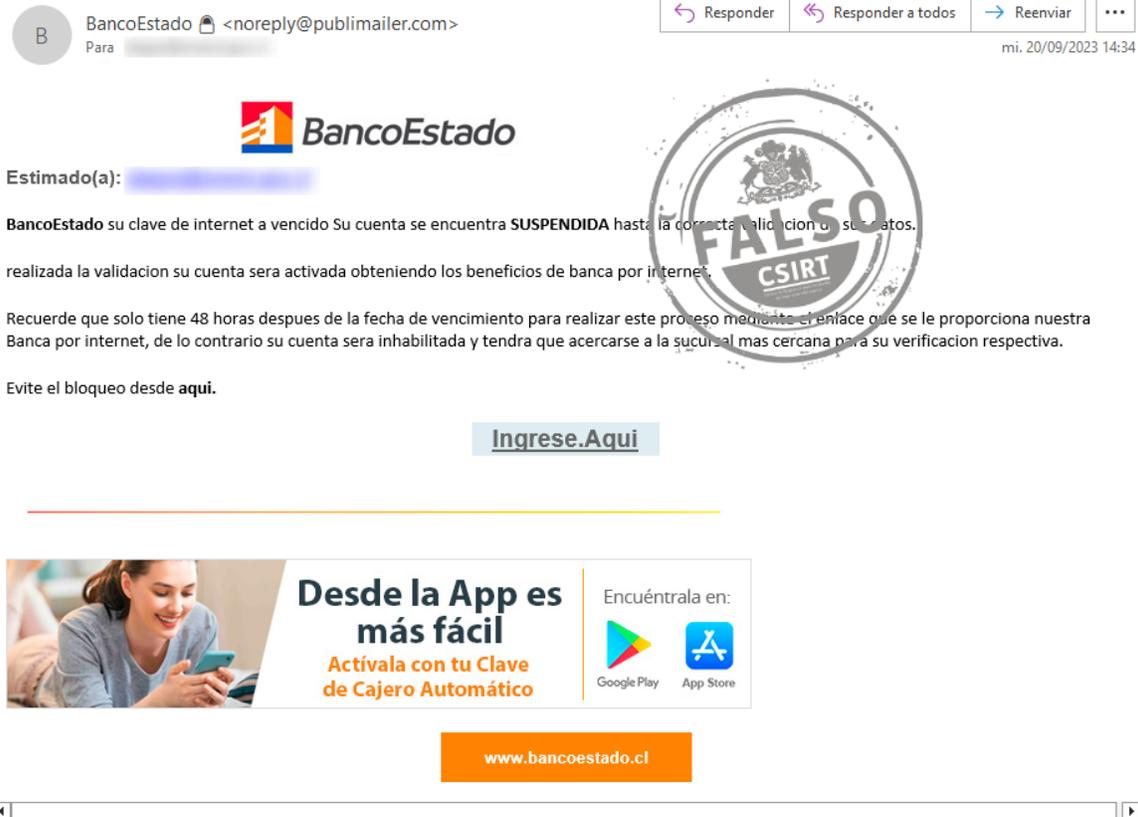
Correos de salida

apache@tapisol.net.net

IP	Comentario
168.232.165.126	SMTP

Imágenes Relacionadas

Aviso Cuenta Temporalmente Suspendida



The screenshot shows an email from BancoEstado with the subject "Aviso Cuenta Temporalmente Suspendida". The email body contains the following text:

BancoEstado su clave de internet a vencido Su cuenta se encuentra **SUSPENDIDA** hasta la correcta validación de sus datos. realizada la validación 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 nuestra Banca por internet, de lo contrario su cuenta sera inhabilitada y tendra que acercarse a la sucursal mas cercana para su verificación respectiva.

Evite el bloqueo desde **aquí**.

[Ingrese.Aquí](#)

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

Encuétrala en:
Google Play App Store

www.bancoestado.cl

A large, semi-transparent watermark with the text "FALSO CSIRT" is overlaid on the right side of the email content.

Imagen 1: Correo Electrónico

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

Alerta de Seguridad Cibernética

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT de Gobierno
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

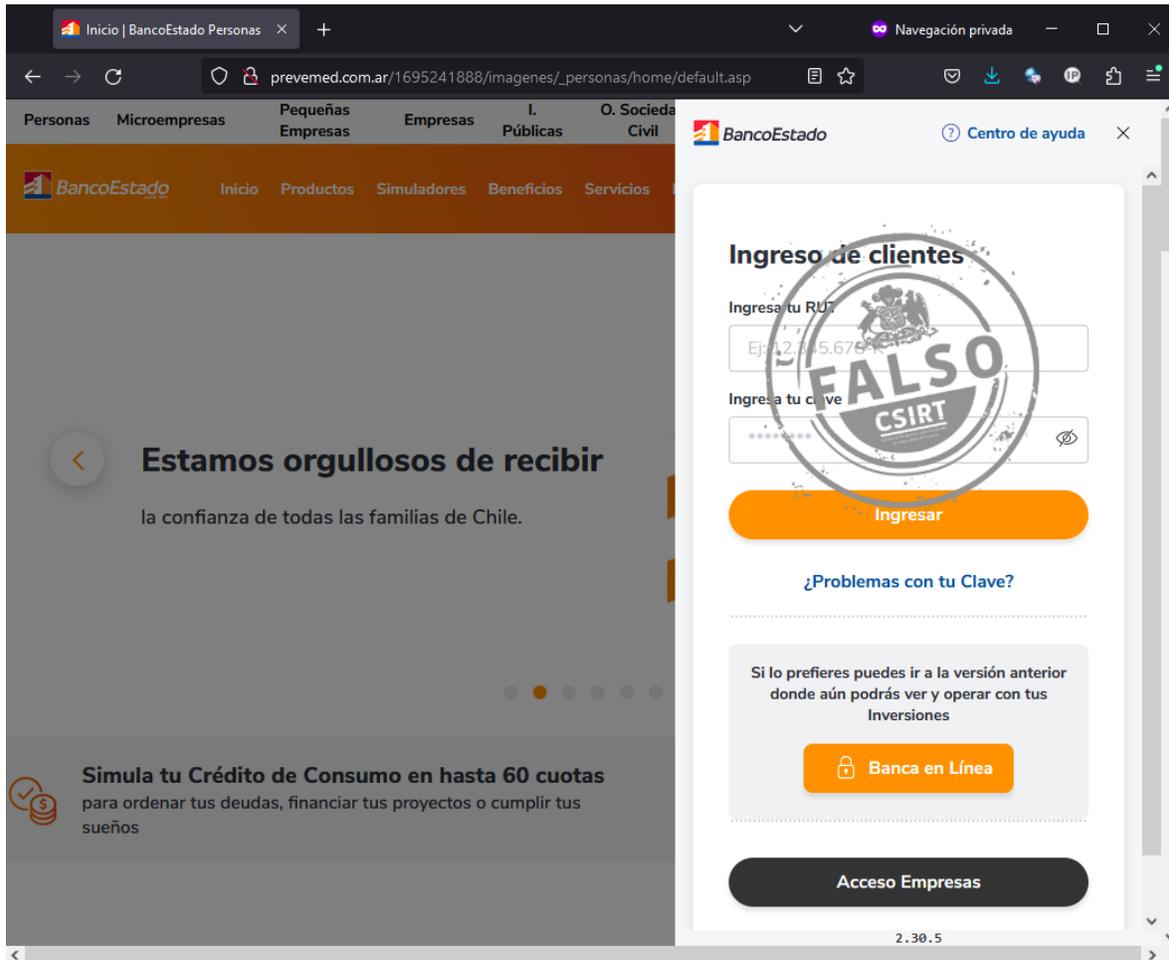


Imagen 2: Sitio fraudulento

CONTACTO Y REDES SOCIALES CSIRT DE GOBIERNO

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>