

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



bAlerta de seguridad cibernética	8FPH24-00922-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de enero de 2024
Última revisión	17 de enero de 2024

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 la que se suplanta a BancoEstado. 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://www.linkedin.com/company/csirt-gob>

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



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

https://patito.sespressx[.]sa.com/1705494947/imagenes/_personas/home/default.asp

URL de redirección

https://procontroltotal[.]com/activacion/cuenta-ajwh/

IP del sitio falso

38.242.247.3

Asuntos del correo electrónico

CUENTA SUSPENDIDA

Correos de salida

apache@mirkifarm.net.net

IP	Comentario
45.7.231.170	SMTP

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>

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

Imágenes Relacionadas

CUENTA SUSPENDIDA



The screenshot shows an email from BancoEstado with the subject 'CUENTA SUSPENDIDA'. The sender is 'BancoEstado <noreply@publemailer.com>' and the recipient is 'iaravenah@interior.gov.cl'. The email text states that the account is suspended and provides instructions for reactivation, including a link to log in. A large circular stamp with the text 'FALSO CSIRT' is overlaid on the right side of the email content.

Responder Responder a todos Reenviar

Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

Estimado(a): iaravenah@interior.gov.cl

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 nuestra Banca. Si no responde lo contrario su cuenta sera inhabilitada y tendra que acercarse a la sucursal mas cercana para su verificacion respectiva.

Evite el bloqueo desde [aquí](#).

[Ingrese.Aqui](#)

www.bancoestado.cl

Atentamente, BancoEstado.

Imagen 1: Correo Electrónico

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>

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

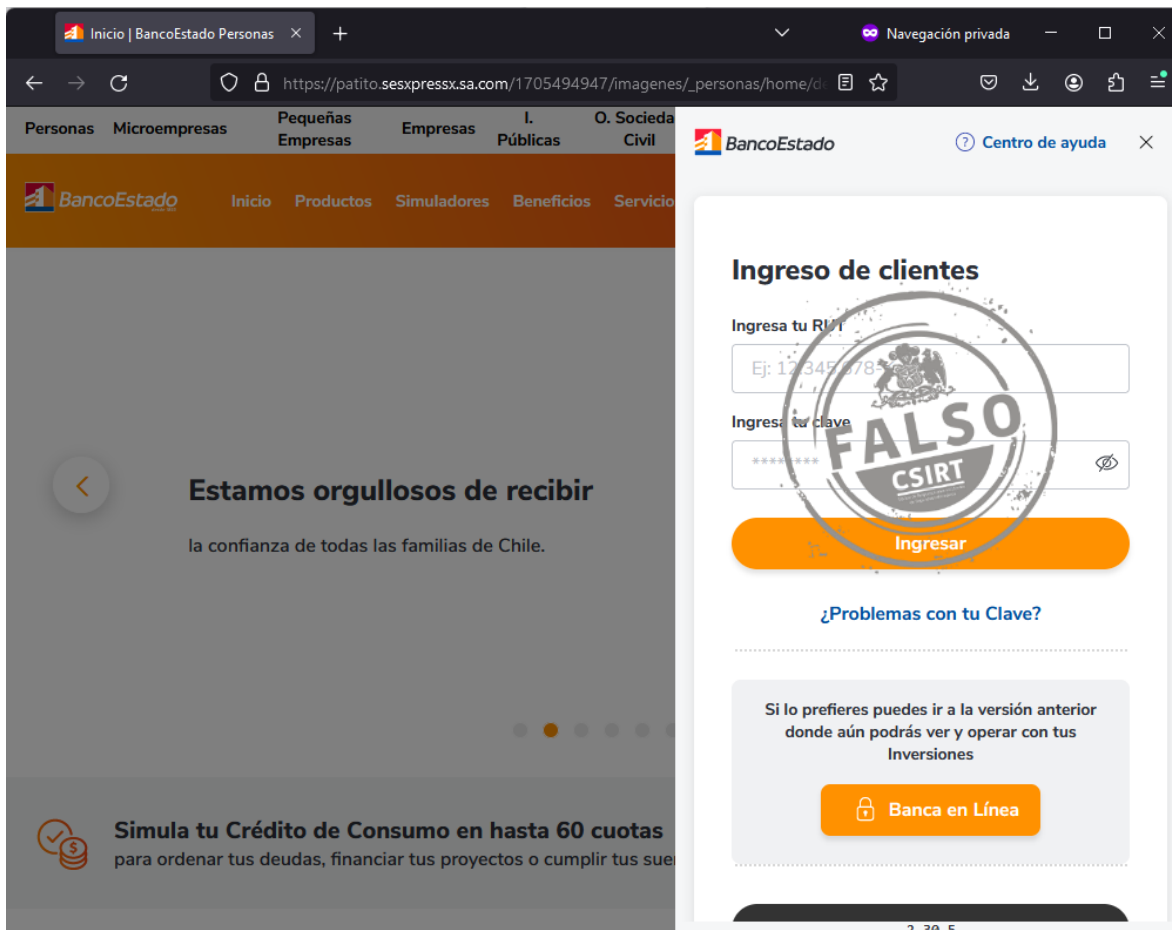


Imagen 2: Sitio fraudulento

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>