

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 | 8FPH23-00895-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 03 de octubre de 2023 |
| Última revisión | 03 de octubre 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, que 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>

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://prsonasantnder[.]bio/1696344931/imagenes/_personas/home/default.asp |
|---|

| |
|---------------------------|
| URL de redirección |
|---------------------------|

| |
|---|
| https://codeundestado[.]com/activacion/cuenta-padw/ |
|---|

| |
|---------------------------|
| IP del sitio falso |
|---------------------------|

| |
|----------------|
| 107.190.131.66 |
|----------------|

| |
|---------------------------------------|
| Asuntos del correo electrónico |
|---------------------------------------|

| |
|--|
| Consulta si tienes pre aprobado un aumento de cupo |
|--|

| |
|--------------------------|
| Correos de salida |
|--------------------------|

| |
|--|
| apache@hdr-nlb8-39c51fa8696874ee.elb.us-east-1.amazonaws.com |
|--|

| IP | Comentario |
|----|------------|
|----|------------|

| |
|----------------|
| 207.246.107.36 |
|----------------|

| IP | Comentario |
|----|------------|
|----|------------|




| |
|------|
| SMTP |
|------|





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

✓ (VALIDACION DE DATOS) Cuenta Suspendida.

 BancoEstado  <noreply@publemailer.com>
Para 

 Responder  Responder a todos  Reenviar 

ma. 03/10/2023 7:50



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 nuestra Banca por internet, de 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](#)







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

Encuétrala en:
 
Google Play App Store

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

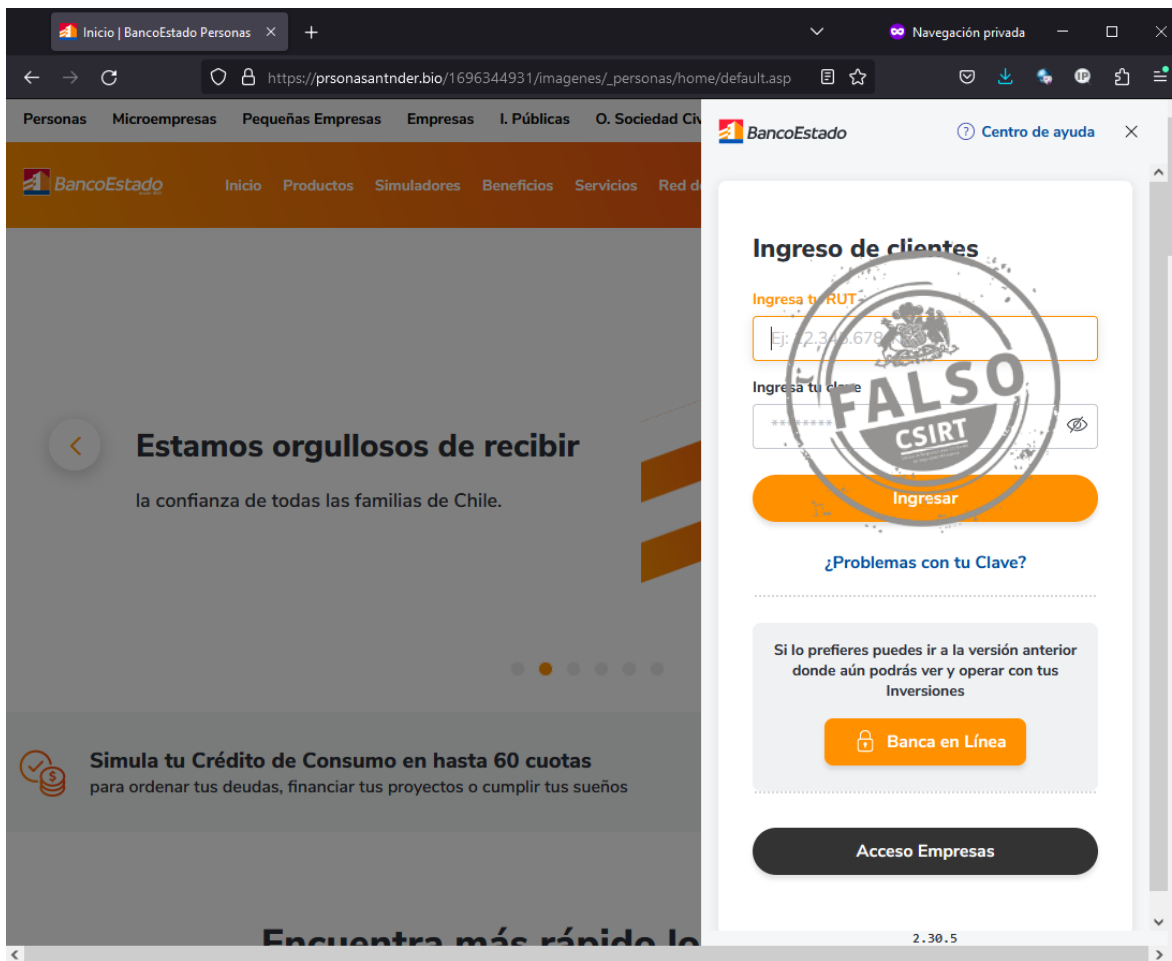


Imagen 2: Sitio fraudulento

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>