

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 informática | 8FPH23-00868-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 03 de agosto de 2023 |
| Última revisión | 03 de agosto 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:

“Santander le informa que ha detectado actividad inusual en su cuenta por lo que hemos suspendido el servicio de su banca hasta actualizar sus datos.”

De abrir el enlace, la persona es dirigida a un sitio falso semejante a los de Banco Santander, donde se expone al robo de su usuario y contraseña (credenciales).

IoC Correo Electrónico

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](#). De forma preventiva, sugerimos aplicar las siguientes [recomendaciones](#) de ciberseguridad.

URL redirección:

[https://homefogastadp\[.\]info/activacion/cuenta-gqgj/](https://homefogastadp[.]info/activacion/cuenta-gqgj/)

URL sitio falso:

[https://n3wfoapecom\[.\]com/1691070100/portada/personas/home.asp](https://n3wfoapecom[.]com/1691070100/portada/personas/home.asp)

Dirección IP del sitio falso:

[64.37.50.122]

CONTACTO Y REDES SOCIALES CSIRT

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

Datos del remitente:

| Asunto | Correo de Salida | SMTP Host |
|--|--------------------------|------------------|
| ✓ FW: (VALIDACION DE DATOS) Cuenta Suspendida. | apache@sermones3.com.com | [190.114.253.52] |

Imagen del mensaje

✓ FW: (VALIDACION DE DATOS) Cuenta Suspendida.

BS Banco Santander <noreply@publimgmail.com>
Para [Redacted]

Responder Responder a todos Reenviar mi. 02/08/2023 22:32



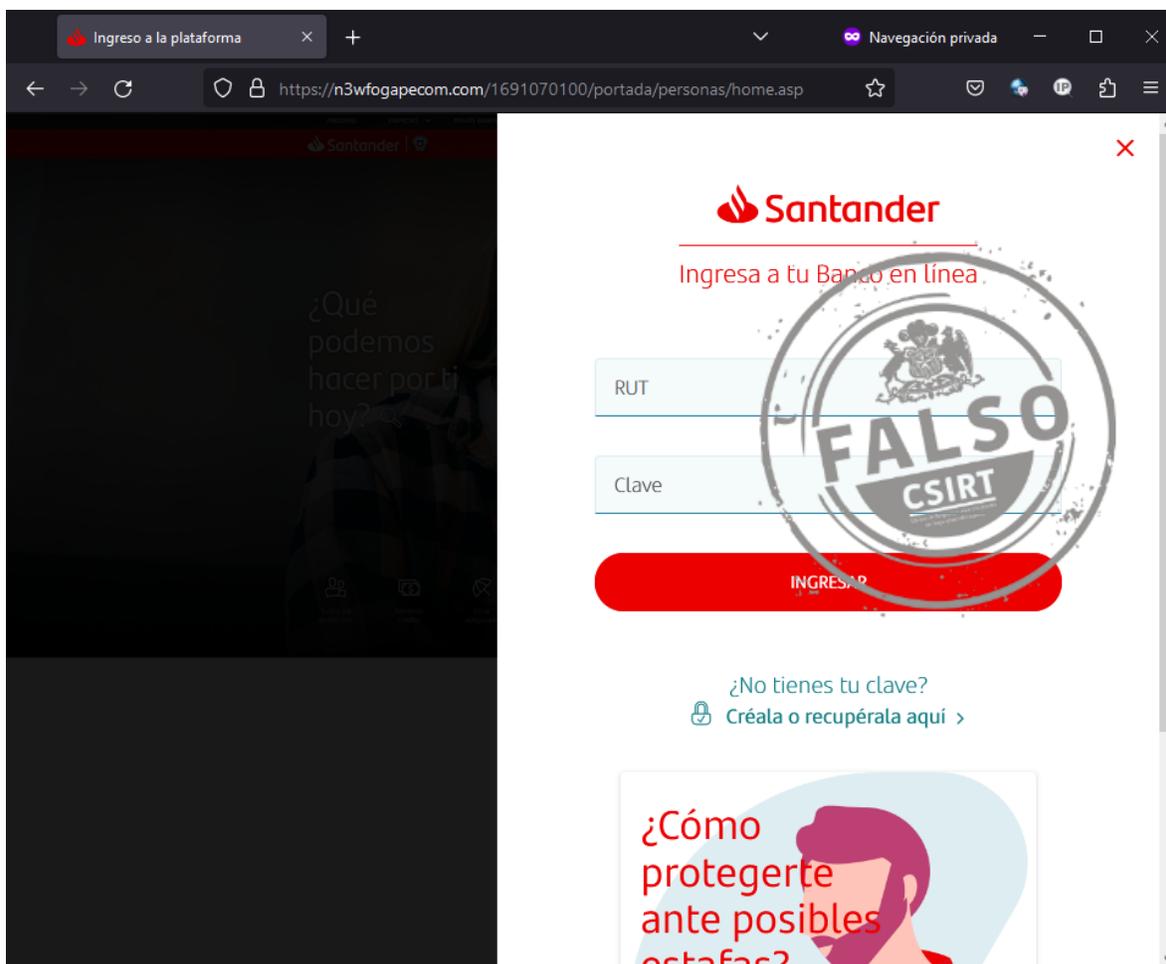
CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: soc@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 del sitio



CONTACTO Y REDES SOCIALES CSIRT

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