

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	8FPH23-00863-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de julio de 2023
Última revisión	27 de julio 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.”*

De abrir el enlace, la persona es dirigida a un sitio falso semejante a los de BancoEstado, 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://avengerpatitos\[.\]com/activacion/cuenta-ezez/](https://avengerpatitos[.]com/activacion/cuenta-ezez/)

URL sitio falso:

[https://xank\[.\]cf/1690465690/imagenes/_personas/home/default.asp](https://xank[.]cf/1690465690/imagenes/_personas/home/default.asp)

Dirección IP del sitio falso:

[162.240.110.92]

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

Datos del remitente:


Asunto	Correo de Salida	SMTP Host
Aviso Cuenta Suspendida	apache@lacayos.net	[45.236.129.99]

Imagen del mensaje

Aviso Cuenta Suspendida

 BancoEstado <noreply@publimgmail.com>
Para [Redacted]

  Responder  Responder a todos  Reenviar 
ju. 27/07/2023 0:48

 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): [Redacted]

BancoEstado su clave de internet a vencido Su cuenta se encuentra **SUSPENDIDA** hasta la correcta validación de sus datos.
realizada la validación su cuenta será activada obteniendo los beneficios de banca por internet.

Recuerde que solo tiene 48 horas después 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 será inhabilitada y tendrá que acercarse a la sucursal más cercana para su verificación respectiva.

Evite el bloqueo desde **aquí**.

[Ingrese.Aquí](#)







www.bancoestado.cl

Atentamente, BancoEstado.



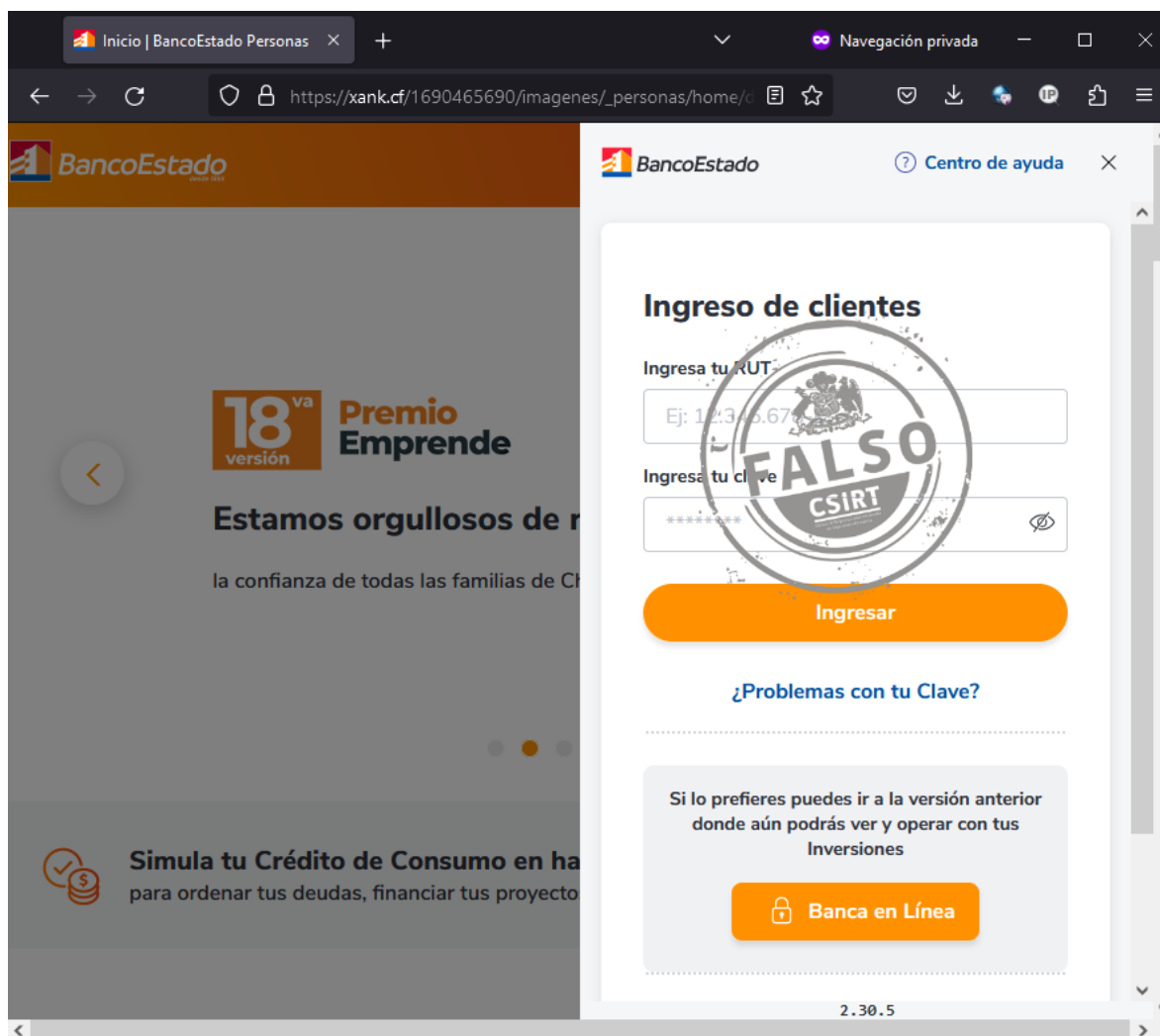
CONTACTO Y REDES SOCIALES CSIRT

 <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>