

Alerta de seguridad informática	8FPH22-00535-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de mayo de 2022
Última revisión	31 de mayo de 2022

## NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una campaña de phishing vía correo electrónico que proviene, supuestamente, del BancoEstado. En esta campaña, los delincuentes indican falsamente a la víctima que su cuenta se encuentra suspendida, debido a que no se ha realizado el proceso de Verificación de Identidad. Para realizar este falso proceso, el atacante dispone de un enlace que dirige a un sitio falso, semejante al de Banco Estado, donde se expone al robo de su usuario y contraseña (credenciales).

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

## Indicadores de compromiso

**URL Redirección:**

[https://noxpro2\[.\]com/activacion/cuenta-taiu/](https://noxpro2[.]com/activacion/cuenta-taiu/)

**Sitio falso:**

[https://cnhrd.tarabgin\[.\]ir/ztkug/pagina/imagenes/comun2008/banca-en-linea-personas.html](https://cnhrd.tarabgin[.]ir/ztkug/pagina/imagenes/comun2008/banca-en-linea-personas.html)

**Asunto:**

CUENTA BLOQUEADA

**Correo de salida:**

apache@21129.bodis[.]com

**SMTP Host:**

[168.232.165.154]

## Otros antecedentes

### Certificado Digital

Fecha Válido	:	17-05-2022
Fecha Término	:	17-05-2023
Emitido	:	PortSwigger CA

### Datos Alojamiento y Dominio

IP	:	[185.51.202.58]
Número de sistema autónomo (AS) IP	:	48715
Etiqueta del sistema autónomo IP	:	Sefroyek Pardaz Engineering Co. LTD
Registrador IP	:	RIPE NCC
País IP	:	IR
Dominio	:	tarabgin[.]ir
Registrador Dominio	:	Tarabgin Co

# Imagen del mensaje



martes 31-05-2022 2:26

BancoEstado <noreply@publemailer.com>

CUENTA BLOQUEADA

Para [redacted].d



Estimado (a) Cliente: [redacted].d

Su cuenta muestra según nuestro sistema un mensaje de error: Error: BCE001547-56, mismo que se define como CUENTA SUSPENDIDA, que se ha generado por que usted no ha realizado el proceso de Verificación de Identidad.

Es necesario que ingrese a nuestra web para poder verificar su información en nuestra base de datos o de lo contrario su servicio de banca por internet quedara bloqueada y sera necesario acudir a nuestra sucursal mas cercana para el desbloqueo de su cuenta.

🏠 Ingresando a [Banco Estado - Activación](#) Usted podrá restablecer el acceso a sus cuentas

[\[ \] \[Activar Cuenta\]](#)

600 200 7000 / [bancoestado.cl](#)

Infórmese sobre la garantía legal de los depósitos en su banco o en [www.cmfchile.d](#)

Este es un correo electrónico generado automáticamente. Por favor no responder.

## Por tu seguridad, sigue estos consejos:

- Nunca compartas tus claves de tarjetas y de acceso a Banca en Línea o Aplicación, ni tus códigos de autorización.
- Siempre ingresa a [www.bancoestado.cl](#), asegurándote que la dirección esté bien escrita.



Conoce más recomendaciones de seguridad de BancoEstado en [www.bancoestado.cl](#)

Síguenos en @bancoestado

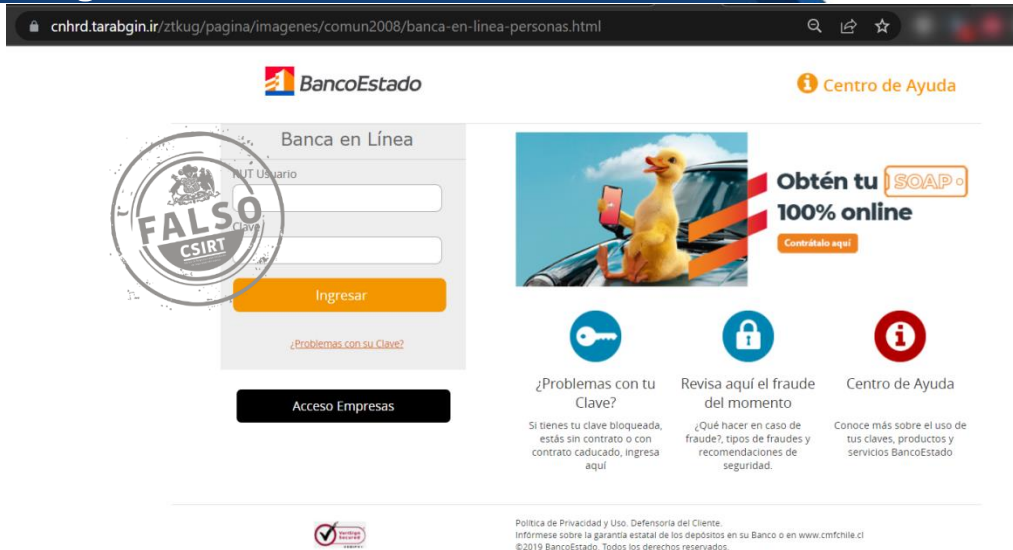


Infórmese sobre la garantía estatal de los depósitos en su banco o en [www.cmfchile.d](#)

De conformidad al artículo 20 B de la Ley 19.496 sobre Protección de los Derechos de los Consumidores, donde se regula el envío de correo masivos. Si usted no quiere recibir nuevos mensajes desde esta dirección, debe pinchar en el link al final de este correo para no recibir nuevos e-mail. Se deja constancia que los datos de contacto de este envío (direcciones, teléfonos, direcciones electrónicas, etc.) son reales y correctos y su e-mail ha sido extraído a través de medios mecánicos o tecnológicos desde nuestras propias bases de datos, sitios públicos de Internet e impresos de publicidad.

© 2019 BancoEstado - todos los derechos reservados.  
Infórmese sobre la garantía estatal de los depósitos en su Banco o en [www.sbif.cl](#)

# Imagen del sitio



## Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.