

Alerta de seguridad informática	8FPH22-00530-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de mayo de 2022
Última revisión	19 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 Banco Estado. En esta campaña, los delincuentes indican falsamente a la víctima que su acceso a la banca en línea por internet expiró de manera temporal, por lo que la cuenta se encuentra inhabilitada hasta validar los datos. Para esto, el atacante dispone de un enlace, el cual 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

**Sitio redirección:**

[https://gestionvalpa\[.\]net/activacion/cuenta-wreo/](https://gestionvalpa[.]net/activacion/cuenta-wreo/)

**Sitio falso:**

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

**Asunto:**

Alerta de Seguridad\_ Dispositivo desconocido.

**Correo de salida:**

apache@21129.bodis[.]com

**SMTP Host:**

[186.64.121.148]

## Otros antecedentes

**Certificado Digital**

Fecha Válido	:	18-05-2022
Fecha Término	:	16-08-2023
Emitido	:	Let's Encrypt R3

**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
País IP	:	IR
Dominio	:	tarabgin[.]ir
Registrador Dominio	:	Tarabgin Co

## Imagen del mensaje



Estimado(a): [Redacted]

**BancoEstado** le comunica que su acceso a la banca en línea por internet ha expirado de manera temporal por lo que su cuenta se encuentra **INHABILITADO** hasta la correcta validación de sus datos.

Realizado este proceso su cuenta será activada de manera inmediata obteniendo los beneficios de la banca por internet de nuestra web BancoEstado.

Recuerde que solo tiene 48 horas de plazo disponible para realizar este proceso de seguridad que le brinda nuestra entidad bancaria. De no proceder con la corrección de sus datos su cuenta será suspendido y tendrá que acercarse a la sucursal más cercana para su verificación respectiva.

Por su seguridad evite el uso incorrecto de terceros y la suspensión de su cuenta.

[Validar Mis Datos](#)



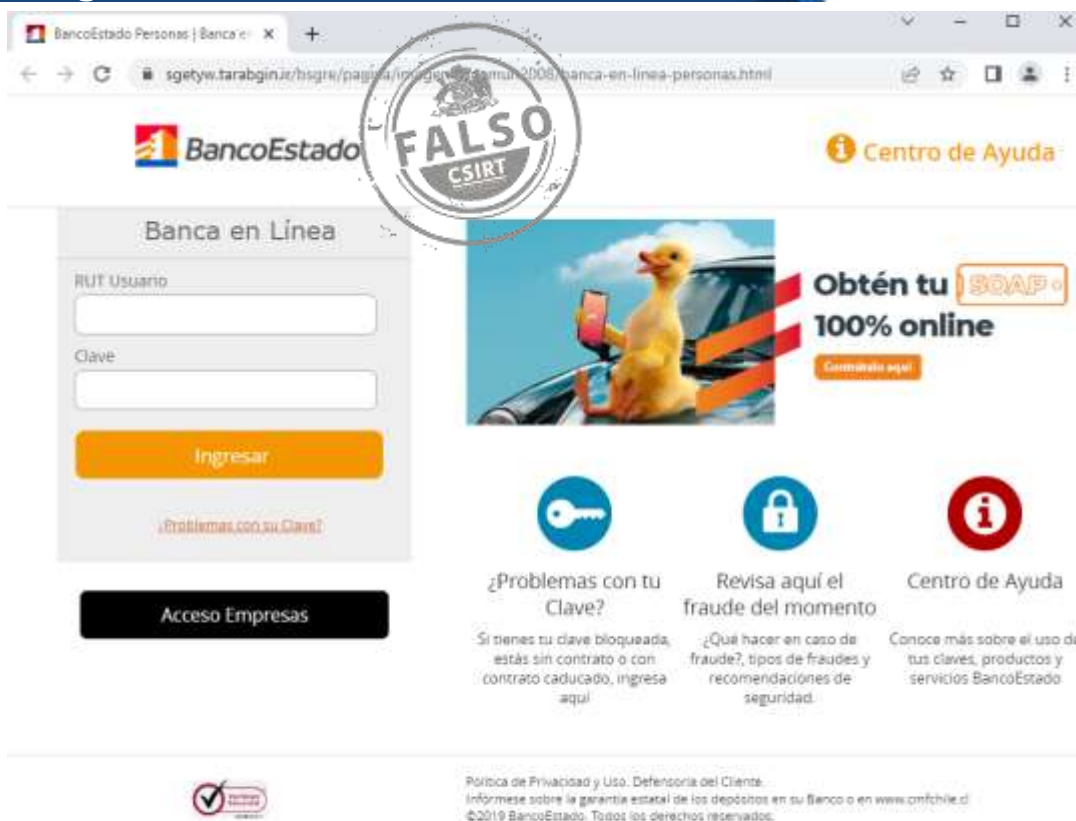
Desde la App es más fácil  
Actívala con tu Clave de Cajero Automático

Encuéntrala en:  
Google Play App Store

[www.bancoestado.cl](http://www.bancoestado.cl)

Atentamente, BancoEstado.

## Imagen del sitio



The image shows a screenshot of the BancoEstado website. A large, semi-transparent watermark with the text "FALSO CSIRT" is overlaid on the page. The website content includes a login form for "Banca en Línea" with fields for "RUT Usuario" and "Clave", an "Ingresar" button, and a link for "Problemas con su Clave?". To the right, there is a promotional banner for "Obtén tu SOAP 100% online" featuring a duck holding a smartphone. Below the banner are three service links: "¿Problemas con tu Clave?", "Revisa aquí el fraude del momento", and "Centro de Ayuda". At the bottom, there is a "Política de Privacidad y Uso" link and a copyright notice for 2019 BancoEstado.

## 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.