

Alerta de seguridad informática	8FPH22-00541-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2022
Última revisión	14 de junio 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 afectada 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 los servidores de procesos bancarios han sido actualizados. Sin embargo, se informa que la persona no tiene su cuenta registrada, por lo que se bloqueó su cuenta de forma temporal. Para reactivar la cuenta, el atacante dispone de un enlace que dirige hacia 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:**

[http://asedl\[.\]am/Servicio\\_Estado/cuenta-tfzg/](http://asedl[.]am/Servicio_Estado/cuenta-tfzg/)

**Sitio falso:**

[https://sixthstartech\[.\]com/Resumen/pagina/imagenes/comun2008/banca-en-linea-personas.html](https://sixthstartech[.]com/Resumen/pagina/imagenes/comun2008/banca-en-linea-personas.html)

**Asunto:**

✓ FW: Cuenta Suspendido (VALIDACION DE DATOS)

**Correo de salida:**

apache@mechaportal[.]com

**SMTP Host:**

[168.232.165.2]

## Otros antecedentes

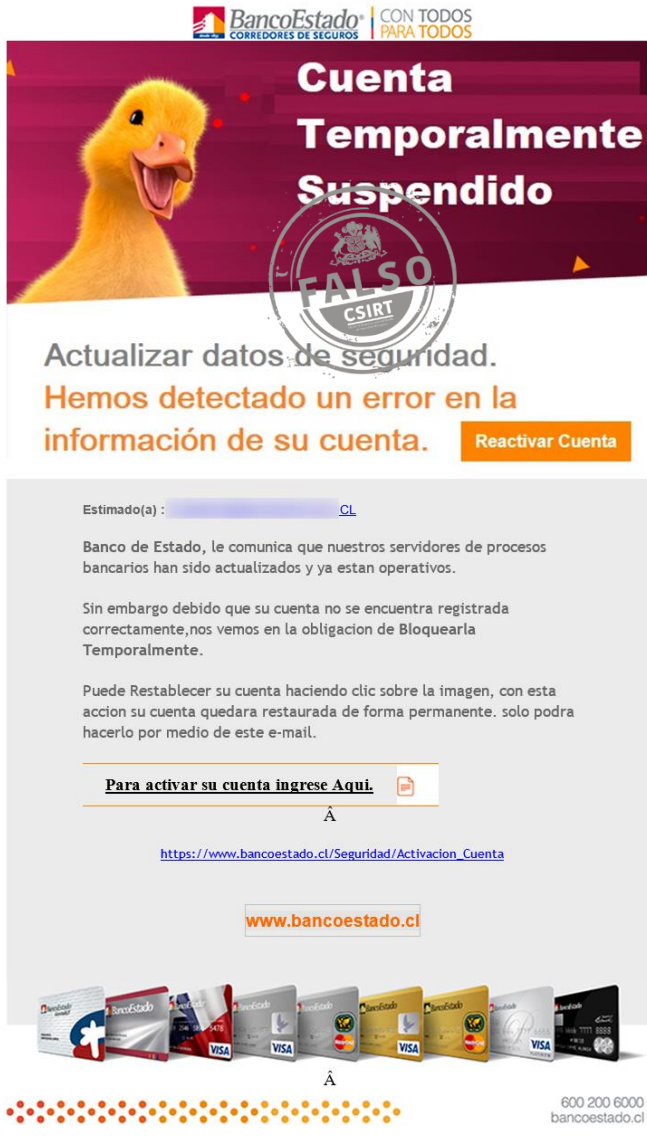
**Certificado Digital**

Fecha Válido	:	12-04-2022
Fecha Término	:	12-07-2022
Emitido	:	cPanel, Inc. Certification Authority

**Datos Alojamiento y Dominio**

IP	:	[192.254.225.27]
Número de sistema autónomo (AS) IP	:	46606
Etiqueta del sistema autónomo IP	:	UNIFIEDLAYER-AS-1
Registrador IP	:	ARIN
País IP	:	US
Dominio	:	asedl[.]am
Registrador Dominio	:	ucom (Ucom LLC)

## Imagen del mensaje



**BancoEstado** | CON TODOS  
CORREDORES DE SEGUROS PARA TODOS

# Cuenta Temporalmente Suspendido

**FALSO**  
CSIRT

Actualizar datos de seguridad.  
Hemos detectado un error en la  
información de su cuenta. [Reactivar Cuenta](#)

Estimado(a) :

Banco de Estado, le comunica que nuestros servidores de procesos bancarios han sido actualizados y ya estan operativos.

Sin embargo debido que su cuenta no se encuentra registrada correctamente, nos vemos en la obligacion de Bloquearla Temporalmente.

Puede Restablecer su cuenta haciendo clic sobre la imagen, con esta accion su cuenta quedara restaurada de forma permanente. solo podra hacerlo por medio de este e-mail.

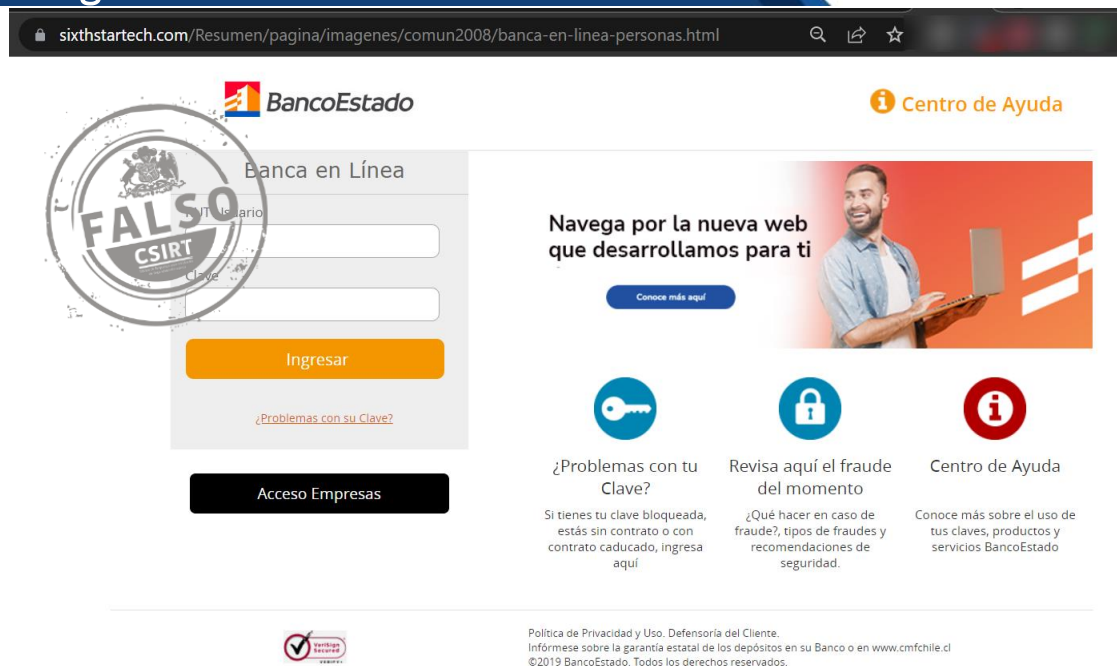
[Para activar su cuenta ingrese Aqui.](#)

[https://www.bancoestado.cl/Seguridad/Activacion\\_Cuenta](https://www.bancoestado.cl/Seguridad/Activacion_Cuenta)

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

600 200 6000  
bancoestado.cl

## Imagen del sitio



The screenshot shows the BancoEstado website. At the top left is the BancoEstado logo. To its right is a 'Centro de Ayuda' link. The main content area is divided into two sections. On the left is the 'Banca en Línea' login form, which includes fields for 'Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. Below the login form is an 'Acceso Empresas' button. A large, semi-transparent watermark with the text 'FALSO CSIRT' is overlaid on the login form. On the right is a promotional banner for the new website, featuring a man with a laptop and the text 'Navega por la nueva web que desarrollamos para ti'. Below the banner are three icons: a key, a padlock, and an information icon. Each icon has a corresponding text block: '¿Problemas con tu Clave?' (with a subtext about blocked keys), 'Revisa aquí el fraude del momento' (with a subtext about fraud types), and 'Centro de Ayuda' (with a subtext about key usage). At the bottom left is a 'Garantía Estatal' logo. At the bottom right is a footer with a privacy policy link and copyright information: 'Política de Privacidad y Uso. Defensoría del Cliente. Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.cmfchile.cl ©2019 BancoEstado. Todos los derechos reservados.'

## 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.