

Alerta de seguridad informática	8FPH22-00544-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de junio de 2022
Última revisión	22 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 afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC 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 IoC 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, de Banco Estado. En esta campaña, los delincuentes indican falsamente a la víctima que los servidores de los procesos bancarios han sido actualizados y que ya están operativos. Sin embargo, debido que la cuenta no se encontraba registrada correctamente, se debió bloquear temporalmente. Para ello, el atacante dispone de un enlace, el cual al ingresar la persona es dirigida 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:

[http://asedl\[.\]am/Servicio_Estado/cuenta-iddb/](http://asedl[.]am/Servicio_Estado/cuenta-iddb/)

Sitio falso:

[https://sixthstartech\[.\]com/Conoce/pagina/imagenes/comun2008/banca-en-linea-personas.html](https://sixthstartech[.]com/Conoce/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	:	[101.53.141.67]
Número de sistema autónomo (AS) IP	:	132420
Etiqueta del sistema autónomo IP	:	282, Sector 19
Registrador IP	:	APNIC
País IP	:	IN
Dominio	:	sixthstartech[.]com
Registrador Dominio	:	PDR Ltd. d/b/a PublicDomainRegistry.com

Imagen del mensaje



martes 21-06-2022 23:34

BancoEstado <noreply@publemailer.com>

✓ FW: Cuenta Suspendido (VALIDACION DE DATOS)

Para: [Redacted] <[Redacted]@[Redacted].cl>

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.



Cuenta Temporalmente Suspendido


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

Estimado(a) : [Redacted] <[Redacted]@[Redacted].cl>

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 Aquí. 

https://www.bancoestado.cl/Seguridad/Activacion_Cuenta

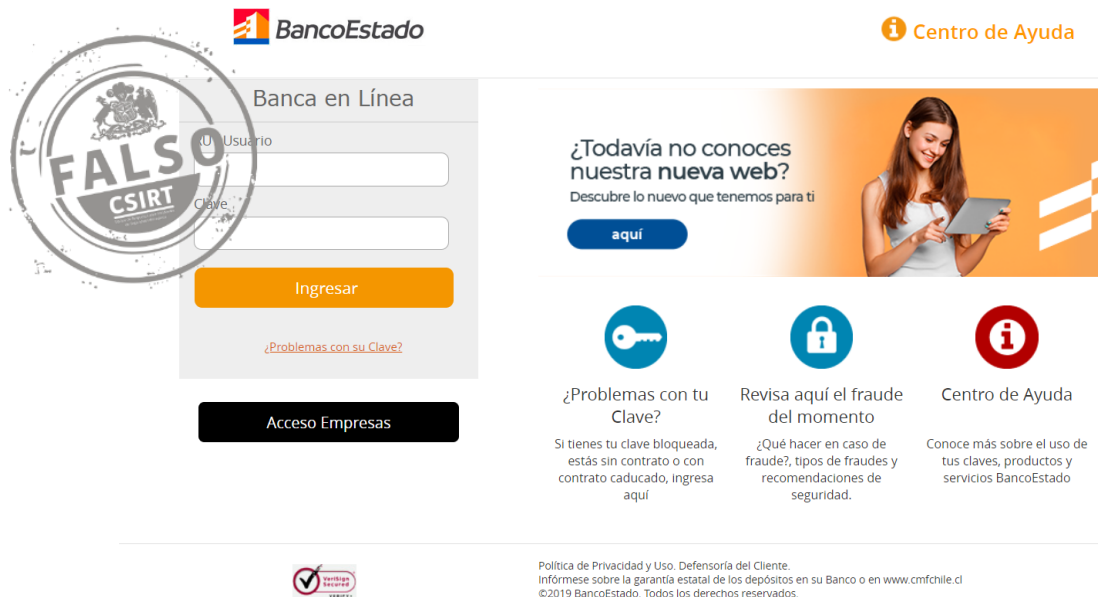
www.bancoestado.cl



600 200 6000
bancoestado.cl

Imagen del sitio

sixthstartech.com/Conoce/pagina/imagenes/comun2008/banca-en-linea-personas.html



The screenshot shows the BancoEstado online banking interface. On the left, there is a login form titled 'Banca en Línea' with fields for 'Usuario' and 'Clave', an 'Ingresar' button, and a link for 'Problemas con su Clave?'. Below the login form is a button for 'Acceso Empresas'. On the right, there is a 'Centro de Ayuda' section with a woman using a tablet. Below this, there are three columns of links: '¿Problemas con tu Clave?' (with a key icon), 'Revisa aquí el fraude del momento' (with a padlock icon), and 'Centro de Ayuda' (with an information icon). At the bottom, there is a 'Verifica seguridad' logo and a privacy policy notice.

BancoEstado Centro de Ayuda

Banca en Línea

Usuario

Clave

Ingresar

[Problemas con su Clave?](#)

Acceso Empresas

¿Todavía no conoces nuestra nueva web?
Descubre lo nuevo que tenemos para ti

[aquí](#)

¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí

Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.

Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado

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.