

Alerta de seguridad informática	8FPH22-00472-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de febrero de 2022
Última revisión	11 de febrero 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 señala falsamente a sus destinatarios que “su clave de internet a vencido y su cuenta se encuentra suspendida hasta la validación de sus datos”.

La víctima, de presionar el enlace, es dirigida a un sitio falso y malicioso semejante al BancoEstado. De esta forma el atacante obtiene sus credenciales.

Observación

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

Indicadores de compromiso

URL sitio redirección:

[http://toybeachclub\[.\]com/activacion/cuenta-tfqr/](http://toybeachclub[.]com/activacion/cuenta-tfqr/)

URL sitio falso:

[http://newcastle.co\[.\]jp/mants/imagenes/comun2008/banca-en-linea-personas.html](http://newcastle.co[.]jp/mants/imagenes/comun2008/banca-en-linea-personas.html)

Asunto:

Cuenta Suspendido (VALIDACION DE DATOS)

Correo Saliente:

[agedefyingskin@host.strykerdigital\[.\]com](mailto:agedefyingskin@host.strykerdigital[.]com)

SMTP Host:

[179.6.252.154]

Otros antecedentes

Certificado Digital

Fecha Valido	:	No aplica
Fecha Término	:	No aplica
Emitido	:	No aplica

Datos Alojamiento y Dominio

IP	:	[1.33.169.198]
Número de sistema autónomo (AS)	:	2514
Etiqueta del sistema autónomo	:	NTT PC Communications, Inc
País	:	JP
Registrador	:	APNIC
Información de registro Dominio	:	New Castle Co., Ltd.
Correo electrónico	:	abuse@namesilo.com

Imagen del mensaje

Cuenta Suspendido (VALIDACION DE DATOS)

BancoEstado <noreply@publemailer.com>
Para: Usted

FALSO CSIRT

 **BancoEstado**

Estimado(a): 82@hotmail.com

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.

Recuerde que solo tiene 48 horas despues 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 sera inhabilitada y tendra que acercarse a la sucursal mas cercana para su verificacion respectiva.

Evite el bloqueo desde **aqui**.

[Ingresa.Aqui](#)

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

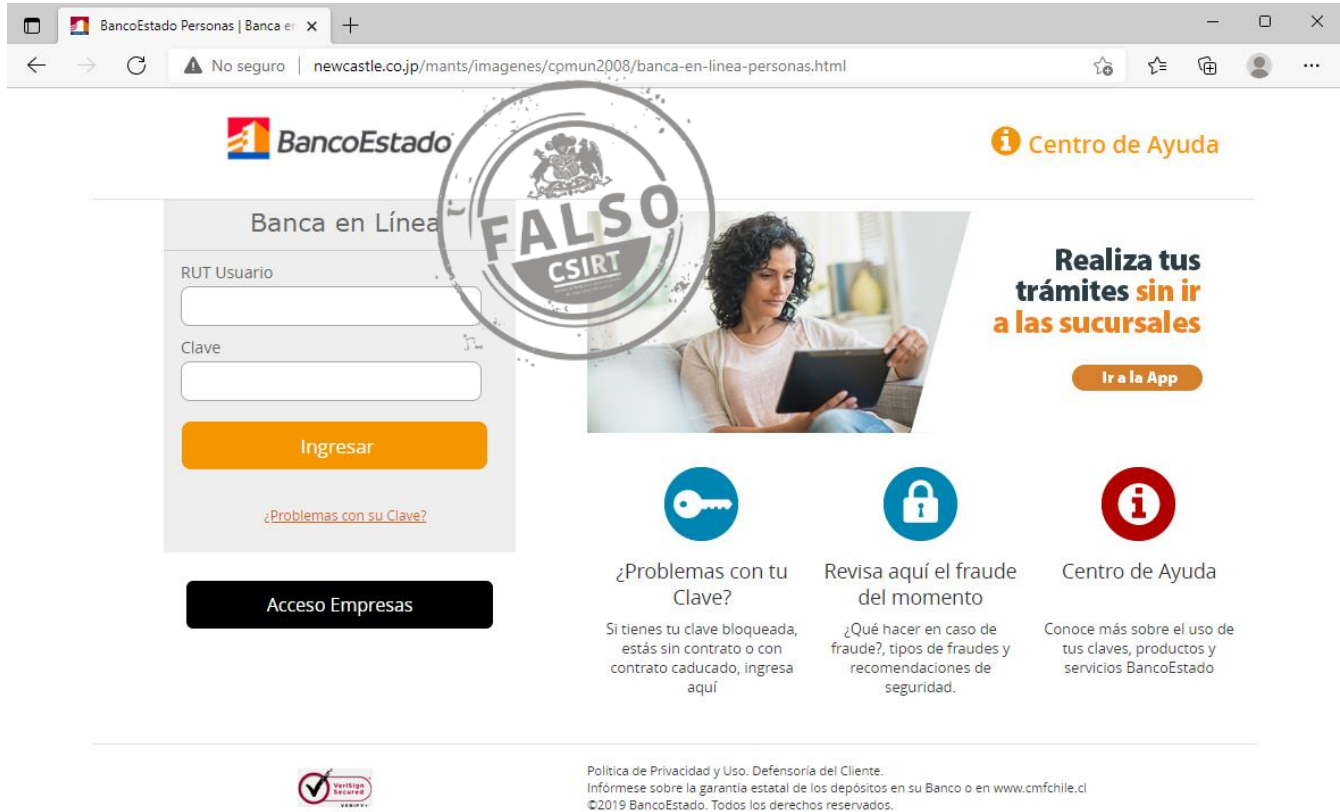
Encuéntrala en:
 
Google Play App Store

www.bancoestado.cl

Atentamente, BancoEstado.

[Responder](#) | [Reenviar](#)

Imagen del sitio



The screenshot shows the BancoEstado website interface. A large, semi-transparent watermark with the text "FALSO CSIRT" and the CSIRT logo is overlaid on the page. The website content includes the BancoEstado logo, a "Centro de Ayuda" link, 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?". Below the login form is an "Acceso Empresas" button. To the right, there is a section titled "Realiza tus trámites sin ir a las sucursales" with an "Ir a la App" button. Further down, there are three columns of links: "¿Problemas con tu Clave?", "Revisa aquí el fraude del momento", and "Centro de Ayuda". At the bottom, there is a "Verificado Seguro" logo and a footer with legal information and copyright notice.

BancoEstado

Centro de Ayuda

Banca en Línea

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)

Acceso Empresas

Realiza tus trámites **sin ir a las sucursales**

Ir a la App

¿Problemas con tu Clave?

Revisa aquí el fraude del momento

Centro de Ayuda

Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí

¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.

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

Verificado Seguro

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.