

Alerta de seguridad cibernética	8FPH20-00252-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Junio de 2020
Última revisión	23 de Junio de 2020

## 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), advierte sobre una campaña de smishing que proviene supuestamente de Banco Estado.

El atacante intenta persuadir a las personas para utilizar un enlace adjunto en el correo.

El mensaje informa que su tarjeta de coordenadas ha caducado.

Al seleccionar el enlace, la persona es dirigida a un sitio falso de Banco Estado, donde se expone al robo de sus credenciales.

## Observación

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

## Indicadores de compromiso

### Urls Redirecciones:

hxxp://bit[.]ly/2zRMMBI?l=www[.]bancoestado[.]cl

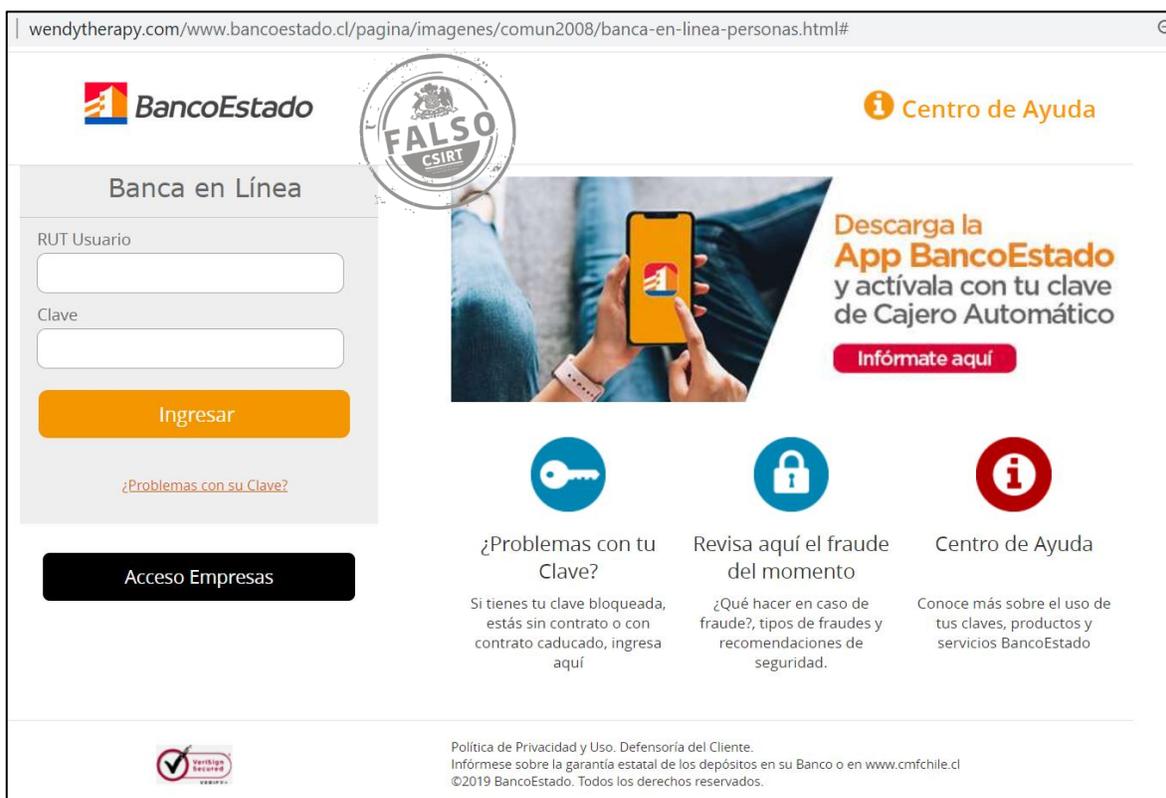
### Urls sitio falso:

hxxp://wendytherapy[.]com/www[.]bancoestado[.]cl/pagina/imagenes/comun2008/banca-en-linea-personas[.]html#

## Imagen del mensaje



## Imagen del sitio



wendytherapy.com/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html#

**BancoEstado**

**Centro de Ayuda**

Banca en Línea

RUT Usuario

Clave

**Ingresar**

[¿Problemas con su Clave?](#)

**Acceso Empresas**

**Descarga la App BancoEstado y actívala con tu clave de Cajero Automático**

**Infórmate 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](http://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.