
Alerta de Seguridad Informática (8FPH-00040-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 26 de Junio de 2019 | Última revisión 26 de Junio de 2019

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 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.

Resumen

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Estado. El correo trata de persuadir a los clientes del Banco indicándoles que por motivos de seguridad han bloqueado clave de acceso a la banca en línea y ofrece la necesidad de que vuelvan a verificar su cuenta, Al hacerlo, se trata de convencer a las personas para que realicen el procedimiento ingresando a los enlaces adjuntos en el correo.

Indicadores de compromisos

Url's:

- <http://www.sac.or.th/en/@/https://www.bancoestado.cl/?cliente=ebernal@interior.gov.cl>
- <https://www2.bancoestado.cl/banca-en-linea.b-estado.com/BancoEstado/?id=ZWJlcm5hbGFAaW50ZXJpb3luZ292LmNs>

Smtip Host

w11.estado-msg[.]co [109.120.151.86]

Subdominio relacionados

f3.estado-msg[.]co [41.79.78.175]

Sender

BancoEstado.cl@w11.estado-msg[.]co

From (Falso):

BancoEstado.cl <BancoEstado.cl@w11.estado-msg[.]co>

Subject:

Servicio de Transferencias bloqueado: *****@*****.cl

Imagen Phishing correo


miércoles 26-06-2019 11:30

BancoEstado.cl <BancoEstado.cl@w11.estado-msg.co>

Servicio de Transferencias bloqueado: @ .cl

Para @ .cl

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

 BancoEstado

Hola @ .cl 26 de Junio de 2019

Servicio de Transferencias Bloqueado

Por motivos de seguridad hemos bloqueado tu Clave de acceso a la Banca en Línea y tu Tarjeta Clave para operar por Internet.


Este bloqueo obedece a una medida preventiva adoptada por el departamento de seguridad de BancoEstado, por este motivo es necesario realizar la verificación solicitada.

Iniciar Verificación

600 200 7000 / bancoestado.cl

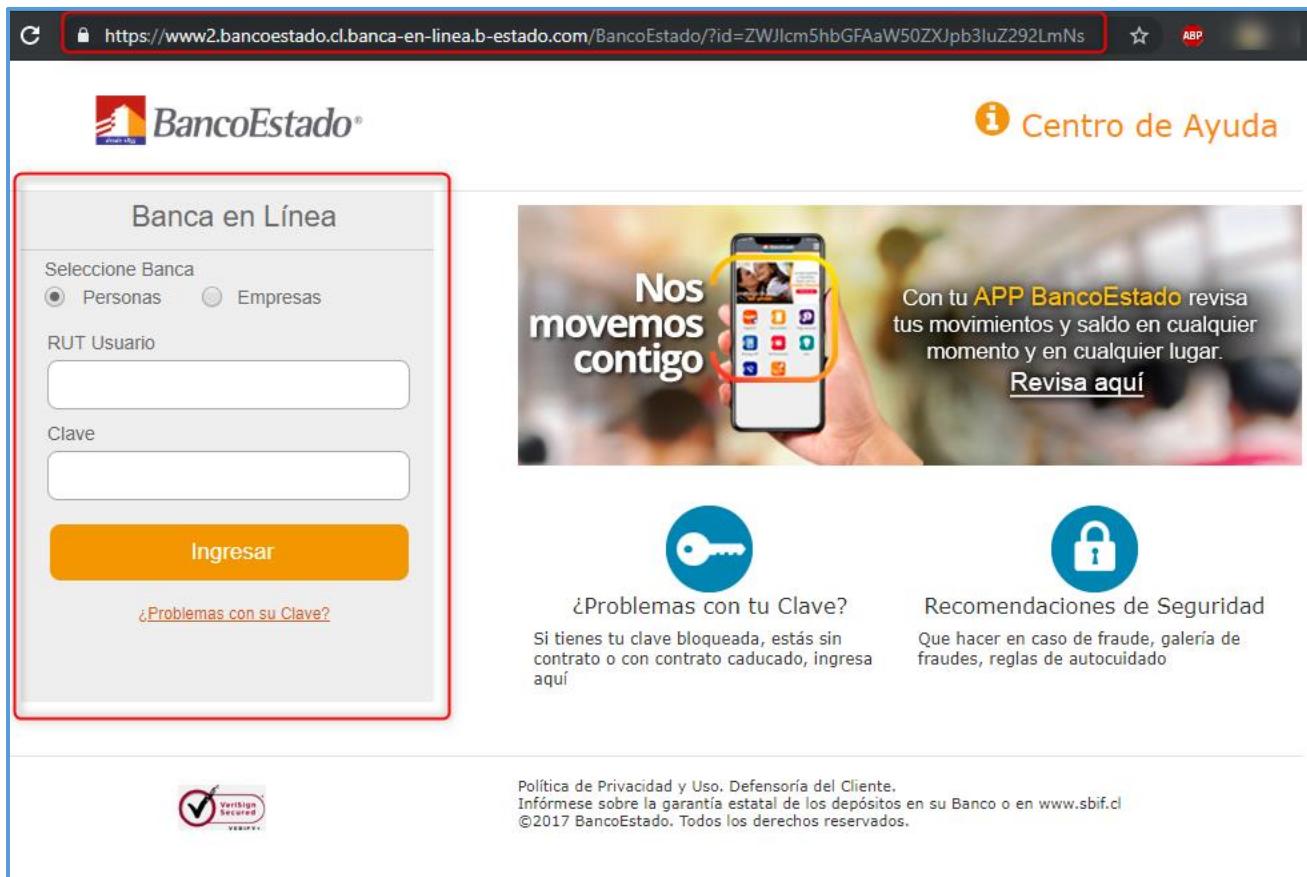
Infórmese sobre la garantía estatal de los depósitos en la Superintendencia de Bancos e Instituciones Financieras de Chile.

Este es un correo electrónico generado automáticamente. Por favor no responder.

 Para un uso seguro de tus **Productos BancoEstado.**

- Si realizas compras por Internet, hazlo en sitios seguros y nunca le entregues los datos de tus tarjetas a terceros.
- Siempre que uses tus tarjetas en los Cajeros Automáticos, asegúrate que no hayan desconocidos a tu alrededor.

Imagen Sitio Phishing




The image shows a screenshot of a phishing website for BancoEstado. The browser's address bar displays the URL: <https://www2.bancoestado.cl.banca-en-linea.b-estado.com/BancoEstado/?id=ZWJlcm5hbGFAaW50ZXJpb3luZ292LmNs>. The website features the BancoEstado logo and a "Centro de Ayuda" link. A red box highlights the login section, which includes a "Banca en Línea" header, radio buttons for "Personas" and "Empresas", input fields for "RUT Usuario" and "Clave", an "Ingresar" button, and a link for "¿Problemas con su Clave?". A central banner promotes the BancoEstado app with the text "Nos movemos contigo" and "Con tu APP BancoEstado revisa tus movimientos y saldo en cualquier momento y en cualquier lugar. Revisa aquí". Below the banner are two links: "¿Problemas con tu Clave?" and "Recomendaciones de Seguridad". The footer contains a Verisign Secure logo, 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.sbif.cl ©2017 BancoEstado. Todos los derechos reservados."

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- 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

Contactos

 <https://www.csirt.gob.cl>

 + (562) 24863850

 @CSIRTGOB

 <https://www.linkedin.com/company/csirt-gob>