

Alerta de seguridad informática	8FPH20-00109-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Febrero de 2020
Última revisión	06 de Febrero 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 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), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente del Banco Estado.

El mensaje informa a la víctima sobre la suspensión de la cuenta producto de la no verificación de identidad. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que al ingresar podrá reestablecer el acceso a la cuenta. Al seleccionar el vínculo la víctima es dirigida a un sitio semejante al del Banco donde se expone al robo de sus credenciales.

Observación

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

Indicadores de compromisos

Urls:

<http://jvali.fcav.unesp.br/Home/linea/>

<http://www.gorbanjara.in/portal/imagenes/comun2008/banca-en-linea-personas.html>

Sender:

apache[.]metalero[.]com

Smtip Host:

[45.236.131.184]

Subject:

Cuenta Suspendida!

Imagen del correo



Cuenta Suspendida!

Banco Estado <bancoestado@plusconsulting.cl>
jue 09/02/2020 3:19

Responder a todos

BancoEstado Centro de Ayuda

Estimado Cliente:

¡Hola! Su cuenta muestra según nuestro sistema un mensaje de error **Error: BC0001547-56** mismo que se define como **CUENTA SUSPENDIDA**, que se ha generado por que usted no ha realizado el proceso de Verificación de Identidad le adjuntamos cartola donde podrá revisar el saldo y movimientos de sus Fondos Mutuos BancoEstado. Para su mayor seguridad, esta información ha sido encriptada, y para abrirla, deberá ingresar como contraseña, los 4 últimos dígitos de su RUT, sin dígito verificador (Ejemplo: Rut 12.345.678-9 + 5678).

Ingresando a **Banco Estado - Activación** Usted podrá restablecer el acceso a sus cuentas

Activar Cuenta

Le saluda atentamente

BancoEstado S.A. Administradora General de Fondos

Invierte en tu futuro ahorrando desde hoy en el Fondo Mutuo Balanceado Perfil C

600 400 7000 / bancoestado.cl

BancoEstado S.A. Administradora General de Fondos es filial de BancoEstado, donde el banco es agente colocador de los diferentes Fondos Mutuos administrados por ella. La rentabilidad o ganancia obtenida en el pasado por estos fondos, no garantiza que ellas se mantengan en el futuro. Los valores de las cuotas de los Fondos Mutuos son variables. Informese de las características e estándares de las Inversiones en Fondos Mutuos, las que se encuentran contenidas en sus reglamentos internos.

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

Para un uso seguro de Cajeros Automáticos.

- Siempre que uses tus tarjetas en los Cajeros Automáticos, protégete con tu mano el ingreso de tu clave.
- Antes de usar el cajero asegúrate de que no existan objetos extraños en el terminal, si no está el cajero, sal de la zona.

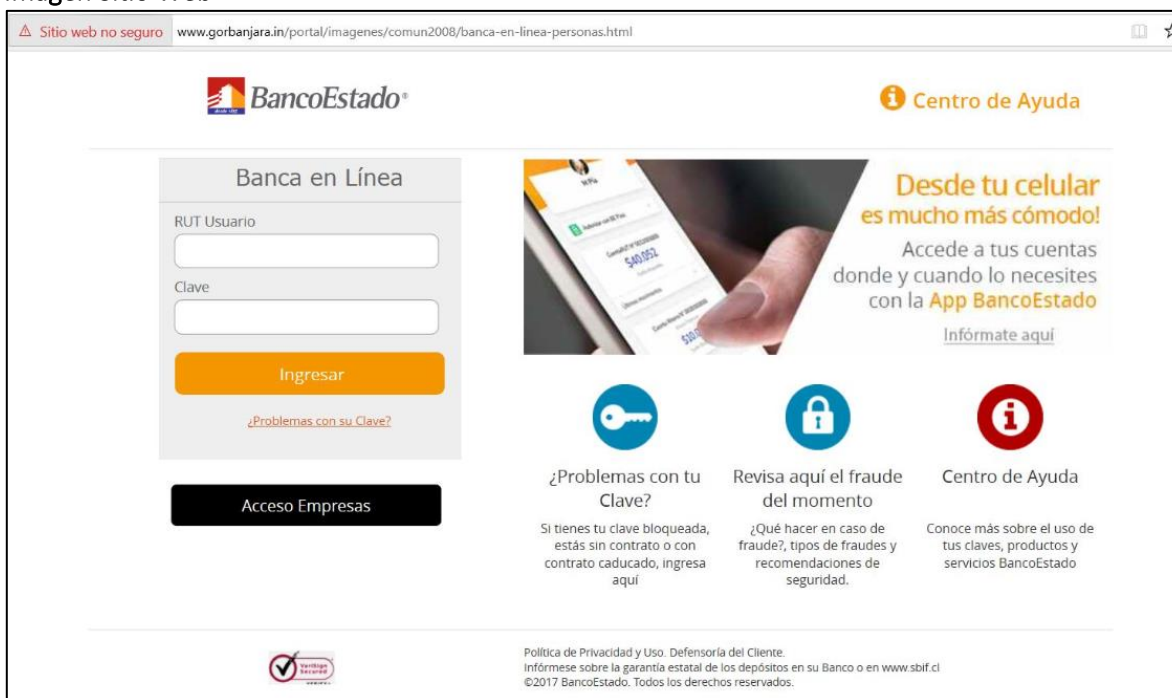
Revisa las recomendaciones de seguridad en www.bancoestado.cl/seguridad

Síguenos en

[@bancoestado](https://twitter.com/bancoestado) [@bancoestado](https://facebook.com/bancoestado) [@bancoestado](https://instagram.com/bancoestado)

De conformidad al artículo 29 B de la Ley 19.640, sobre Protección de los Derechos de los Consumidores, donde se regula el envío de correo masivos, te saludamos y queremos recibir tus comentarios desde esta dirección. Antes de hacer clic en el botón de esta correo para recibir nuestros mensajes. Se debe expresar la conformidad que los datos de contacto de correo electrónico, teléfono, dirección electrónica, así como nombre y apellido que se envía a este correo electrónico a través de medios electrónicos o tecnológicos, desde nuestra página bases de datos, sitios y páginas de Internet e impresión de publicidad.

Imagen Sitio Web



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y 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
- Visualizar los sitios web que se ingresen que sean los oficiales