
Alerta de Seguridad Informática (8FPH-00043-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 12 de Julio de 2019 | Última revisión 12 de Julio 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 se realizó un mantenimiento en sus servicios y se encontró un error en su cuenta, motivo por el cual se procedió al bloqueo temporal de la cuenta. Los criminales tratan de persuadir al usuario de seleccionar el link adjunto para restablecer la cuenta y así obtener las credenciales de acceso. Al seleccionar el enlace se redirige a la víctima a un sitio semejante al de Banco Estado.

“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”

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

- <http://www.x8clothing.co.id/text/Activacion.php>
- <http://graphicox.com/wp-content/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html>

Smtip Host

- 110-170-232-163.static.asianet.co.th [110.170.232.163]
- sia.mediaf.jp [183.177.238.19]

Sender

- www-data@hosting2.bsru.ac.th
- apache@sia.mediaf.jp

Subject:

- Fwd:Cuenta Bloqueada.

Imagen Phishing correo



BancoEstado Notificaciones <noreply@bancoestado.cl>

Fwd: Aviso - Cuenta Bloqueada.



Estimado(a)

Tenemos una información **importante para usted.**

Le informamos que hoy se realizó un mantenimiento en nuestro Servicio (Caja Vecina, ServiEstado, Pagos en Línea). Encontramos error en su cuenta.

Su Cuenta no está Registrada correctamente y la **Bloqueamos Temporalmente**.

Puede Restablecer su cuenta haciendo clic en el siguiente enlace, con esta acción su cuenta quedará Restaurada de forma correcta. solo podrá hacerlo por medio de este e-mail.

[www.bancoestado.cl/Restauracion de Cuenta](http://www.bancoestado.cl/Restauracion%20de%20Cuenta)

En caso de dudas o consultas, contáctenos llamando al **600 200 7000**.

Saluda atentamente,

BancoEstado.

600 200 7000

Imagen Sitio Web

No seguro | graphicox.com/wp-content/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html




The screenshot shows the BancoEstado website interface. At the top left is the BancoEstado logo. To its right is a 'Centro de Ayuda' link. The main content area is divided into two columns. The left column is titled 'Banca en Línea' and contains a login form with fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. Below the form is a button for 'Acceso Empresas'. The right column features a promotional banner for the BancoEstado app, stating 'Somos más de 3 millones usando la App BancoEstado' with a 'Compruébalo aquí' button. Below the banner are three service cards: '¿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). Each card includes a brief description of the service. At the bottom left is a 'Verificar Estado' icon, and at the bottom right is a footer with legal 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
- Visualizar los sitios web que se ingresen que sean los oficiales

Contactos

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

 + (562) 24863850

 @CSIRTGOB

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