
Alerta de Seguridad Informática (8FPH-00044-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 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 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.

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 proceso de actualización en sus servidores, sin embargo su cuenta se encuentra bloqueada temporalmente y para restablecerla debe hacer clic en un enlace (imagen) para así activar su cuenta inmediatamente.

El mensaje establece que solo se puede realizar este procedimiento con el hipervínculo señalado en el correo, de esta forma los criminales tratan de persuadir a al usuario a realizar clic en el hipervínculo de la imagen, solicitando las credenciales de acceso. Este enlace redirige a la víctima a un sitio falso 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:

- [https://helloiloa\[.\]gg/MicroEmpresas/beneficios/](https://helloiloa[.]gg/MicroEmpresas/beneficios/)
- [http://3dprintsibiu\[.\]ro/js/Team/imagenes/comun2008/banca-en-linea-personas\[.\]html](http://3dprintsibiu[.]ro/js/Team/imagenes/comun2008/banca-en-linea-personas[.]html)

Smtip Host

- pr0mart[.]net [170.239.86.133]
- Vicky[.]net [170.239.86.154]

Sender

- apache@pr0mart[.]net
- apache@vicky[.]net

Subject:

- Fwd:Cuenta Bloqueada.

Imagen Phishing correo



BancoEstado  <noreply@bancoestado.cl>

✓ Fw: Cuenta Bloqueado




Estimado(a) :

Banco de Estado, le comunica que nuestros servidores de procesos bancarios han sido actualizados y ya estan operativos.

Sin embargo debido que su cuenta no se encuentra registrada correctamente, nos vemos en la obligacion de Bloquearla Temporalmente.

Puede Restablecer su cuenta haciendo clic sobre la imagen, con esta accion su cuenta quedara restaurada de forma permanente. solo podra hacerlo por medio de este e-mail.

Para activar su cuenta ingrese Aqui. 

https://www.bancoestado.cl/Seguridad/Activacion_Cuenta

www.bancoestado.cl



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 the 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 login form is a black 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 circular icons: a key, a padlock, and an information icon. Each icon is accompanied by a heading and a short paragraph: '¿Problemas con tu Clave?' (with a note about blocked keys), 'Revisa aquí el fraude del momento' (with a note about fraud types), and 'Centro de Ayuda' (with a note about app usage). At the bottom left is a 'Verificado' seal, and at the bottom right is a small footer with privacy policy information and copyright notice.

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>