

Alerta de seguridad informática	8FPH-00051-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Julio de 2019
Última revisión	29 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.

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 que intenta engañar a los usuarios del Banco de Estado. El correo informa a las víctimas que se realizó un mantenimiento en los servicios del banco y producto de ello, se encontró un error en la cuenta del usuario. Lo anterior obligó al bloqueo de la cuenta, y la única forma de activarla nuevamente es seleccionando el enlace indicado en el correo. De este modo, el atacante intenta convencer al usuario para ingresar al enlace y entregar sus credenciales en un sitio semejante al del banco.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

[http://visinet\[.\]tech/readme/Simuladores/](http://visinet[.]tech/readme/Simuladores/)

[http://peacefoundation\[.\]co\[.\]in/fast/imagenes/comun2008/banca-en-linea-personas\[.\]html](http://peacefoundation[.]co[.]in/fast/imagenes/comun2008/banca-en-linea-personas[.]html)

Smtip Host

hwsrv-549720[.]hostwinddns[.]com [142[.]11[.]214[.]245]

From:

apache@hwsrv-549720[.]hostwinddns[.]com

Subject:

Aviso Importante: Alerta Maxima de Seguridad

Imagen Phishing Correo

✓ Aviso Importante: Alerta Maxima de Seguridad

BancoEstado  <bancoestado@plusconsulting.cl>

 CON TODOS PARA TODOS


Vive con tranquilidad.

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. 

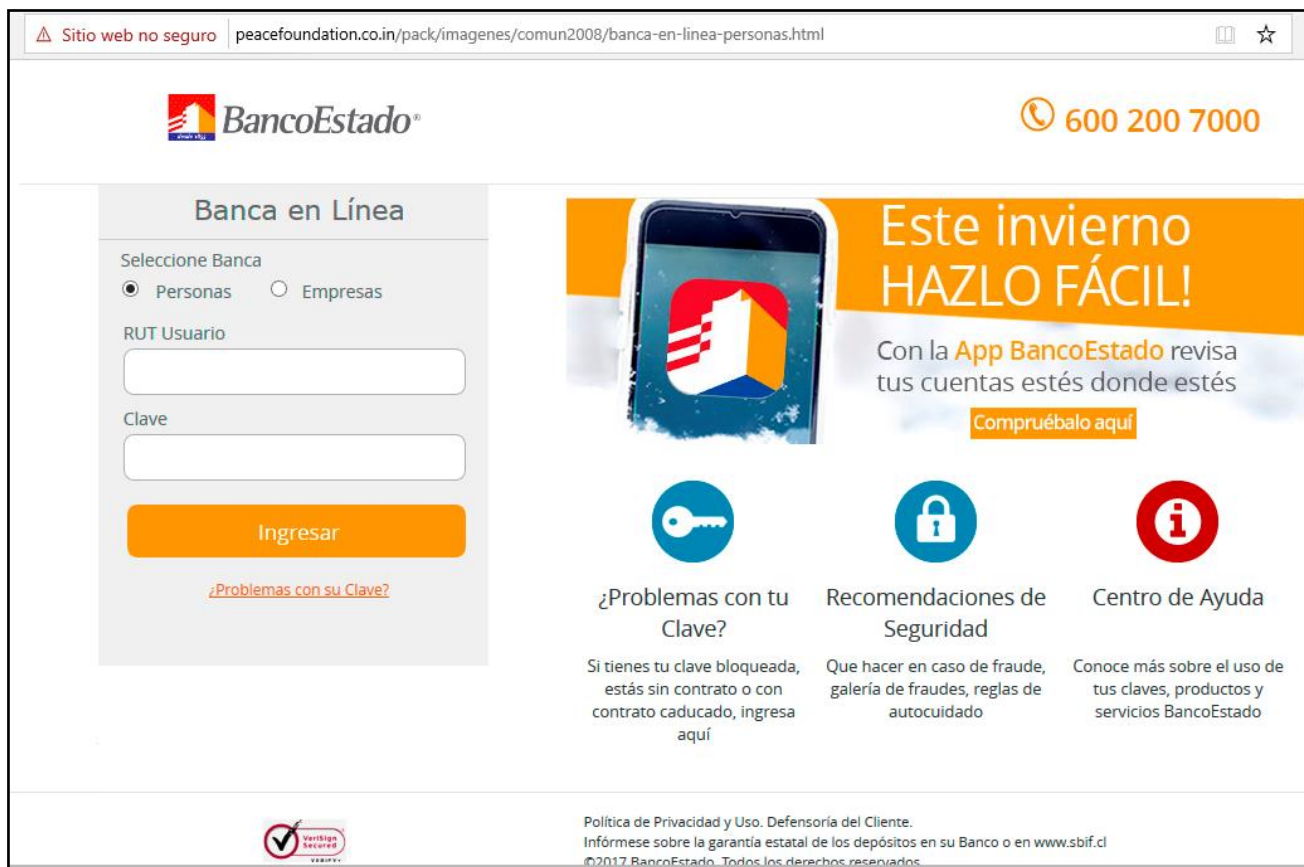
https://www.bancoestado.cl/Seguridad/Activacion_Cuenta

www.bancoestado.cl



600 200 6000
bancoestado.cl

Imagen Sitio Web



Sitio web no seguro | peacefoundation.co.in/pack/imagenes/comun2008/banca-en-linea-personas.html

BancoEstado 600 200 7000

Banca en Línea

Seleccione Banca

Personas Empresas

RUT Usuario

Clave




Ingresar


[¿Problemas con su Clave?](#)

Este invierno HAZLO FÁCIL!

Con la **App BancoEstado** revisa tus cuentas estés donde estés

[Compruébalo aquí](#)

-  **¿Problemas con tu Clave?**
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
-  **Recomendaciones de Seguridad**
Que hacer en caso de fraude, galería de fraudes, reglas de autocuidado
-  **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.sbif.cl ©2017 BancoEstado. Todos los derechos reservados.

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