

Alerta de seguridad cibernética	8FPH20-00148-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Marzo de 2020
Última revisión	30 de Marzo 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 afecta 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), advierte sobre una campaña de phishing que se está difundiendo a través de correos electrónicos falsos que aparentan provenir del Banco Estado.

Los correos asociados a esta campaña tienen ligeras variaciones en sus asuntos, pero en todos los casos explican al cliente que fue detectada una inconsistencia en los registros del banco respecto a la propia cuenta o de algún servicio asociado, razón por la cual, se procedió al bloqueo de ésta. Para desbloquear la cuenta, el atacante disponibiliza un enlace en el cuerpo del correo, el cual lleva la víctima hasta un sitio similar al del banco donde se expone a la pérdida de sus credenciales bancarias.

OBSERVACIÓN

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

INDICADORES DE COMPROMISO

Urls Redirecciones:

[http://torneonet\[.\]site/Activacion/cuenta-utii/](http://torneonet[.]site/Activacion/cuenta-utii/)
[http://Operacoin\[.\]com/Activacion/cuenta-nnid/](http://Operacoin[.]com/Activacion/cuenta-nnid/)

Urls sitio falso:

[http://noukymas\[.\]com/make/imagenes/comun2008/banca-en-linea-personas\[.\]html](http://noukymas[.]com/make/imagenes/comun2008/banca-en-linea-personas[.]html)
[http://sondeclo\[.\]com/damp/imagenes/comun2008/banca-en-linea-personas\[.\]html](http://sondeclo[.]com/damp/imagenes/comun2008/banca-en-linea-personas[.]html)

Smtip Host

186[.]64[.]123[.]161
186[.]64[.]123[.]133
186[.]64[.]123[.]109
186[.]64[.]123[.]111
186[.]64[.]123[.]10
176[.]223[.]129[.]162
45[.]236[.]130[.]21
45[.]7[.]231[.]225
45[.]7[.]231[.]221
45[.]7[.]231[.]168
45[.]7[.]231[.]109

Sender

apache[@]crater[.]net
apache[@]scavin0[.]net[.]net
apache[@]league[.]com
apache[@]intensa[.]net
apache[@]cargos[.]com
apache[@]concierto[.]com
apache[@]dork[.]com
apache[@]tola[.]com
apache[@]unionflor[.]com
apache[@]silfo[.]com

Asunto

Fw: Cuenta Bloqueada
Fw: Cuenta Suspendido
Fw: Cuenta Temporalmente Bloqueada.
Aviso Importante: Cuenta Bloqueado

IMAGEN DEL MENSAJE

De: BancoEstado <bancoestado@plusconsulting.cl>
Para: [Redacted]
CC:
Asunto: Fw: Cuenta Bloqueada

Estimado(a): [Redacted]

Banco de Estado, le comunica que se realizo un mantenimiento en nuestros Servicios(Caja Vecina,ServiEstado.APP). Nuestro sistema ha detectado una inconsistencia catastral en su cuenta.

Debido a este suceso y en cumplimiento con la nueva normativa vigente de seguridad nos vemos en la obligación de **Bloquear su Cuenta**.

Su Cuenta se activara solo por este E-mail: [click aqui](#)

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

www.bancoestado.cl
600 200 7000



Si no deseas continuar recibiendo correos de BancoEstado, por favor haz [click aqui](#)

De: BancoEstado <bancoestado@plusconsulting.cl>
Para: [Redacted]
CC:
Asunto: Fw: Cuenta Suspendido

Estimado(a): [Redacted]

Banco de Estado, le comunica que se realizo un mantenimiento en nuestros Servicios(Caja Vecina,ServiEstado.APP). Nuestro sistema ha detectado una inconsistencia catastral en su cuenta.

Debido a este suceso y en cumplimiento con la nueva normativa vigente de seguridad nos vemos en la obligación de **Bloquear su Cuenta**.

Su Cuenta se activara solo por este E-mail: [click aqui](#)

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

www.bancoestado.cl
600 200 7000



Si no deseas continuar recibiendo correos de BancoEstado, por favor haz [click aqui](#)

De: BancoEstado <bancoestado@plusconsulting.cl>
Para: [Redacted]
CC:
Asunto: Aviso Importante: Cuenta Bloqueado

Estimado(a) [Redacted]

Banco de Estado, le comunica que se realizo un mantenimiento en nuestros Servicios(Caja Vecina,ServiEstado.APP). Nuestro sistema ha detectado una inconsistencia catastral en su cuenta.

Debido a este suceso y en cumplimiento con la nueva normativa vigente de seguridad nos vemos en la obligacion de **Bloquear su Cuenta**.

Su Cuenta se activara solo por este E-mail: [click aqui](#)

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

www.bancoestado.cl
600 200 7000



Si no deseas continuar recibiendo correos de BancoEstado, por favor haz click aqui

De: BancoEstado <bancoestado@plusconsulting.cl>
Para: [Redacted]
CC:
Asunto: Fw: Cuenta Temporalmente Bloqueada.

Estimado cliente: [Redacted]

BancoEstado necesita verificar su Tarjeta De Coordinadas registrado en nuestra banca por Internet, esta operacion requiere ser atendida para poder ingresar a sus cuentas afiliadas a BancoEstado en linea.

Tenemos la incertidumbre de que su cuenta haya podido ser tomado por un tercero. Debido a que la proteccion y seguridad de su cuenta corre por nuestra parte, hemos limitado el acceso en linea de modo temporal, esta medida es tomada con eventualidad en caso de proteccion y es levantado un Reporte del Mismo. [ID243-048.017](#).

El numero de su
comprobante de Operacion
es: **AD-001-3072**.

**Para actualizar tus datos de
manera segura haz click en
el boton Ingresar.**

Tarifado Productos y Tasas de Interes
Politica de Privacidad - Guia del Cliente Bancario (SEIF)
Codigo de Conducta y Buenas Practicas de Bancos e Instituciones Financieras
Informese sobre la garantia estatal de los depositos en su Banco o en www.abif.cl Año 2020
BancoEstado.cl Todos los derechos reservados.

***Recuerde que el hacer caso omiso de este mensaje puede poner en riesgo la seguridad de tu cuenta.**

IMAGEN DEL SITIO



noukymas.com/make/imagenes/comun2008/banca-en-linea-personas.html

BancoEstado Centro de Ayuda

Banca en Línea

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)

Atreverse está en tus manos!

Infórmate aquí

FALSO CSIRT

- 

¿Problemas con tu Clave?

Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
- 

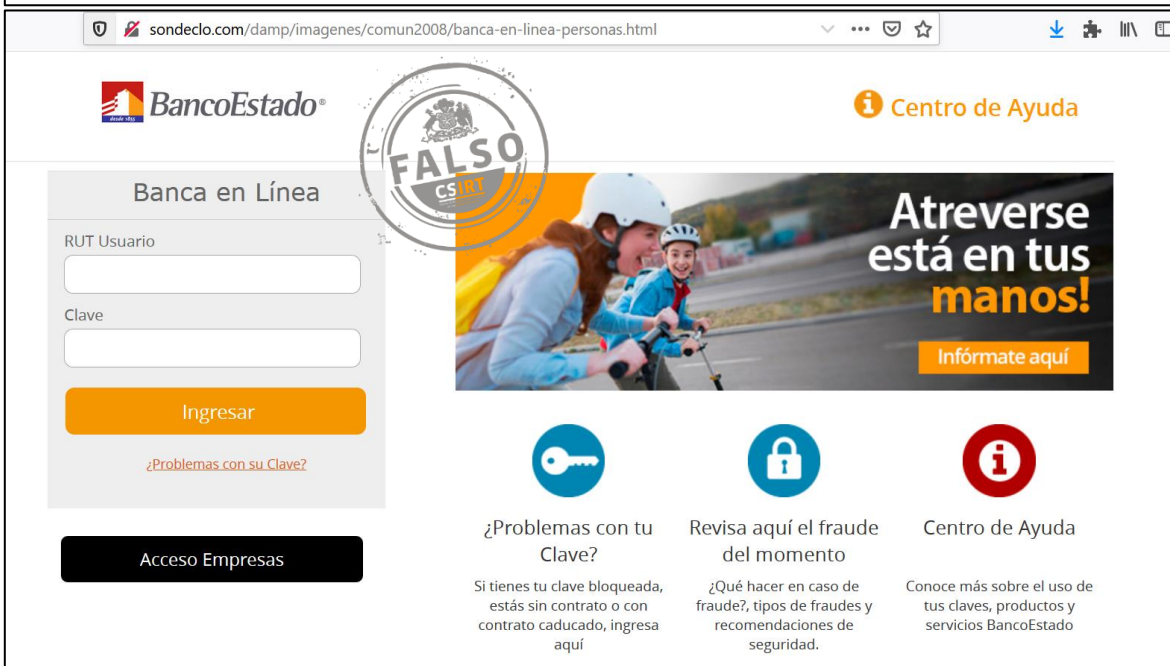
Revisa aquí el fraude del momento

¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
- 

Centro de Ayuda

Conoce más sobre el uso de tus claves, productos y servicios BancoEstado

Acceso Empresas



sondeclo.com/damp/imagenes/comun2008/banca-en-linea-personas.html

BancoEstado Centro de Ayuda

Banca en Línea

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)

Atreverse está en tus manos!

Infórmate aquí


FALSO CSIRT

- 

¿Problemas con tu Clave?

Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
- 

Revisa aquí el fraude del momento

¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
- 

Centro de Ayuda

Conoce más sobre el uso de tus claves, productos y servicios BancoEstado

Acceso Empresas

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 sean los oficiales.