

Alerta de seguridad informática	8FPH-00074-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Noviembre de 2019
Última revisión	13 de Noviembre 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.

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 cuyo mensaje intenta engañar a los usuarios del Banco de Chile. El atacante utiliza varios mensajes en el cuerpo del correo para persuadir al usuario para que seleccione un enlace, siendo direccionado a un sitio semejante al del banco. De esta forma los estafadores podrían capturar las credenciales bancarias de los clientes. A continuación se detallan algunos de los mensajes con los que se intenta engañar a los usuarios.

- Bloqueo de su tarjeta de débito por una compra sospechosa
- Se realizó un descuento porque existió un error
- Se realizó una retención por una deuda
- Se bloqueó una transacción por ser sospechosa

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

[https://is\[.\]gd/dg02v1?skpelk=1ca670c7a5f07a3faf9f59ea42a3429e](https://is[.]gd/dg02v1?skpelk=1ca670c7a5f07a3faf9f59ea42a3429e)

[https://is\[.\]gd/qvc2fu?dxvxwf=a8348663afc1b70f37995dcf09edc633](https://is[.]gd/qvc2fu?dxvxwf=a8348663afc1b70f37995dcf09edc633)

[https://is\[.\]gd/F3jQZ0?luklxg=42ef88bd6393652b698f98c2967824ff](https://is[.]gd/F3jQZ0?luklxg=42ef88bd6393652b698f98c2967824ff)

[https://midoritogo\[.\]com/lbancobechileportallogin1n/2jiht0vqc7/0xauf_prsona/lgin_b5k0/ed2q46/login9uk7/](https://midoritogo[.]com/lbancobechileportallogin1n/2jiht0vqc7/0xauf_prsona/lgin_b5k0/ed2q46/login9uk7/)

Smtip Host

vps31733nl[.]hyperhost[.]name[185.174.172.250]

vps31730nl[.]hyperhost[.]name[185.174.172.222]

vps31735nl[.]hyperhost[.]name[185.174.173.22]

vps31736nl[.]hyperhost[.]name[185.174.173.65]

vps31737nl[.]hyperhost[.]name[185.174.173.104]

vps31731nl[.]hyperhost[.]name[185.174.172.244]

vps31729nl[.]hyperhost[.]name[185.174.172.216]

vps31732nl[.]hyperhost[.]name[185.174.172.248]

vps31728nl[.]hyperhost[.]name[185.174.172.209]

vps31742nl[.]hyperhost[.]name[185.174.173.132]

vps31559nl[.]hyperhost[.]name[185.174.172.87]

Subject:

Aprobar Transaccion

Bloqueo de Compra

Compra Dudosa

Detalle por descuento

Detalle por retención

Deuda cancelada

Imagen Phishing Correo

Banco de Chile

Notificacion Banco de Chile

Estimado : **CLIENTE**
Banco de Chile le informa de una TRANSACCION SOSPECHOSA el dia 05/11/2019 / 18:14:33 .

Puede BLOQUEARLA si usted no lo ha realizado. **BLOQUEAR TRANSACCION.**


 Mi Banco


 Mail


 SMS

 Twitter



 @banchiles

 www.facebook.com/banchiles.cl

 Fonobank 500 456 209

Por tu seguridad este mensaje esta verificado por nuestro equipo de seguridad de Banco de Chile.

Además:

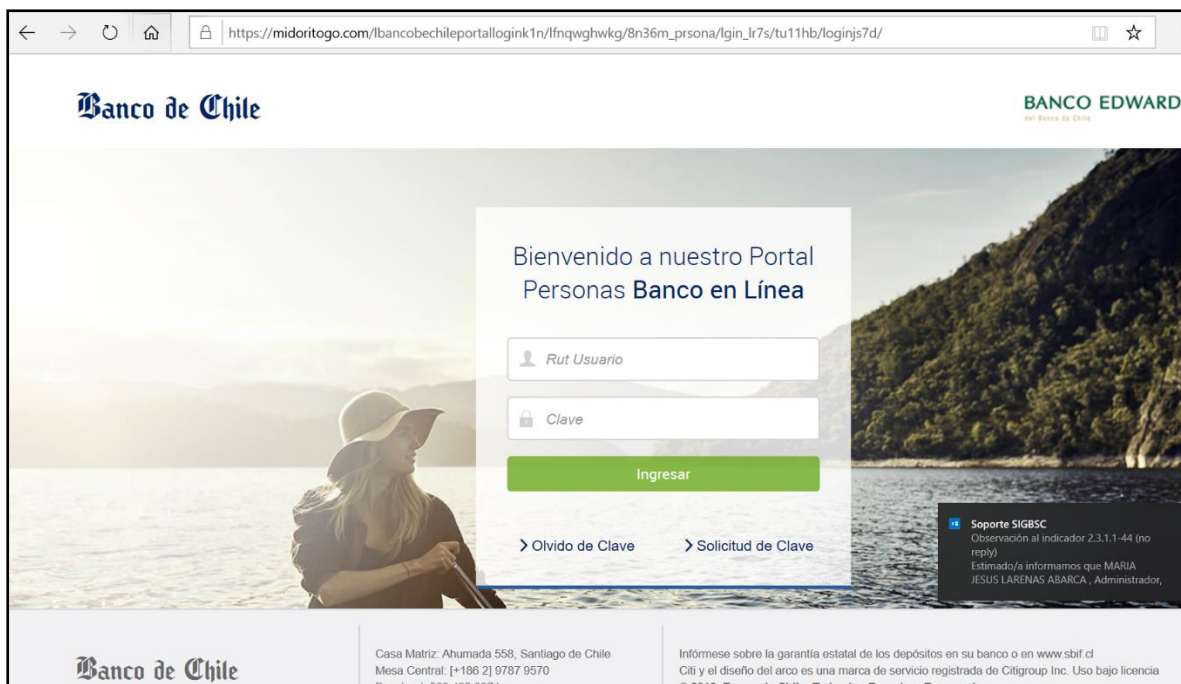
- Este email esta verificado por nuestro equipo de seguridad.
- Nunca le pediremos sus datos por llamada, sms , solamente por esta via.
- Banco de Chile le Mantiene informado de las nuevas modalidades de estafa.
- Siempre le mantendremos Informado con nuestras alertas via correo.
- Los link generados por Banco de Chile son seguros y confiables.
- Nuestros Canales de atencion estan disponibles las 24 horas .

 **SU CLAVES CLAVE**

Este mensaje ha sido enviado con informacion exclusiva para clientes del Banco.

Casa Matriz: Pena 111, Santiago de Chile.
Informese sobre la garantia estatal de los depositos en su banco o en www.sbf.cl 2018.
Todos los derechos reservados.

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