

Alerta de seguridad cibernética	8FPH20-00255-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio 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 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), advierte sobre una campaña de smishing en la que se suplanta al Banco de Chile.

El atacante intenta persuadir a la víctima para utilizar un enlace adjunto.

El mensaje informa que la DigiPass del usuario no está sincronizada, situación que debe ser solucionada para evitar bloqueos.

Al seleccionar el enlace, la persona es dirigida a un sitio falso de Banco de Chile, donde se expone al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Urls Redirecciones:

<https://bancoenlinea.bchile-alerta.com>

Urls sitio falso:

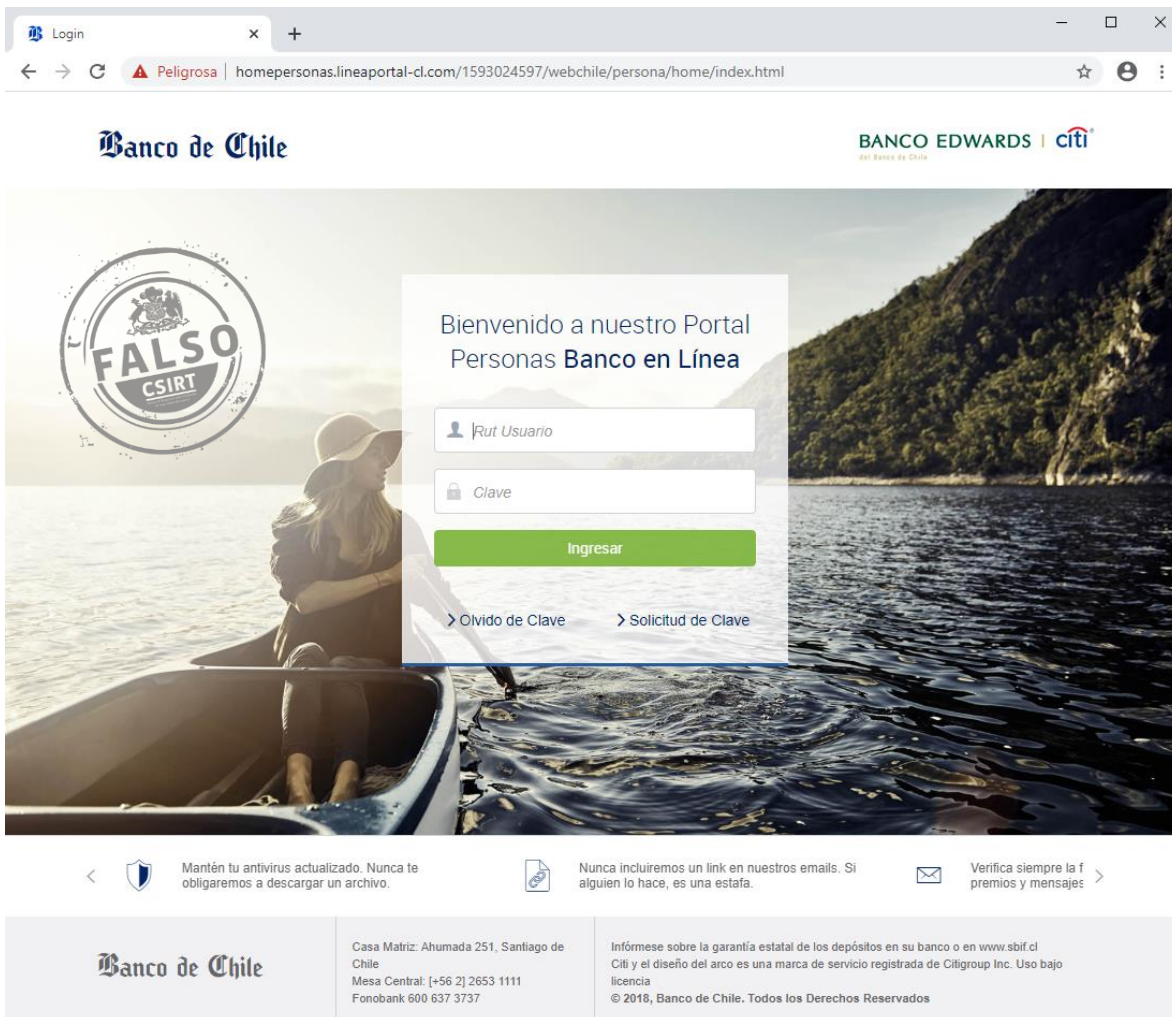
[https://homepersonas.lineaportal-cl\[.\]com/](https://homepersonas.lineaportal-cl[.]com/)

Imagen del mensaje

Banco de Chile - DigiPass
desincronizado, soluciona
inconvenientes y evita
bloqueos, actualice datos aqui:
<https://bancoenlinea.bchile-alerta.com>



Imagen del sitio



Login x +

← → ↻ Peligrosa | homepersonas.lineaportal-cl.com/1593024597/webchile/persona/home/index.html ☆ ⌵ ⋮

Banco de Chile

BANCO EDWARDS | citi
del Banco de Chile

Bienvenido a nuestro Portal
Personas Banco en Línea

Rut Usuario

Clave

Ingresar

> Olvido de Clave > Solicitud de Clave

Mantén tu antivirus actualizado. Nunca te obligaremos a descargar un archivo.

Nunca incluiremos un link en nuestros emails. Si alguien lo hace, es una estafa.

Verifica siempre la f... premios y mensajes >

Banco de Chile

Casa Matriz: Ahumada 251, Santiago de Chile
Mesa Central: [+56 2] 2653 1111
Fonobank 600 637 3737

Infórmese sobre la garantía estatal de los depósitos en su banco o en www.sbif.cl
Citi y el diseño del arco es una marca de servicio registrada de Citigroup Inc. Uso bajo licencia
© 2018, Banco de Chile. Todos los Derechos Reservados

Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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.