

Alerta de seguridad Cibernética	8FPH20-00282-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Agosto de 2020
Última revisión	07 de Agosto 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 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 Smishing se está difundiendo, la que supuestamente proviene del Banco Chile.

El atacante intenta persuadir a la víctima para utilizar un enlace en el mensaje.

El mensaje indica que una supuesta operación bancaria asociada la retiro del 10% de la AFP fue realizada exitosamente y el enlace se ofrece como alternativa para revisar el detalle.

Al seleccionar el link el usuario es dirigido a un sitio falso 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:

hxxps://info-afp.netpersonascl[.]com

### Urls sitio falso:

hxxps://home-bancochilemovil.clsesion[.]com/1596806048/webchile/persona/home/index.html

### Texto Mensaje:

BancoChile - Se ha registrado con éxito tu solicitud de retiro máximo de 10% de AFP. Consulte saldo y movimiento

## Otros antecedentes

## URL Body SHA-256

2f4fd12509daa7d172a71dccacc1ccaaaec1ad42c98ebec434fe69f065dc37f

## Certificado Digital

Fecha Valido : 05/08/2020  
Fecha Termino : 04/11/2020  
Emitido : cPanel, Inc. Certification Authority

## Datos Alojamiento

IP : 80.208.225.239  
Número de sistema autónomo (AS) : AS 62282  
Etiqueta del sistema autónomo : UAB Rakrejus  
País : Lituania  
Registrador : RIPE NCC

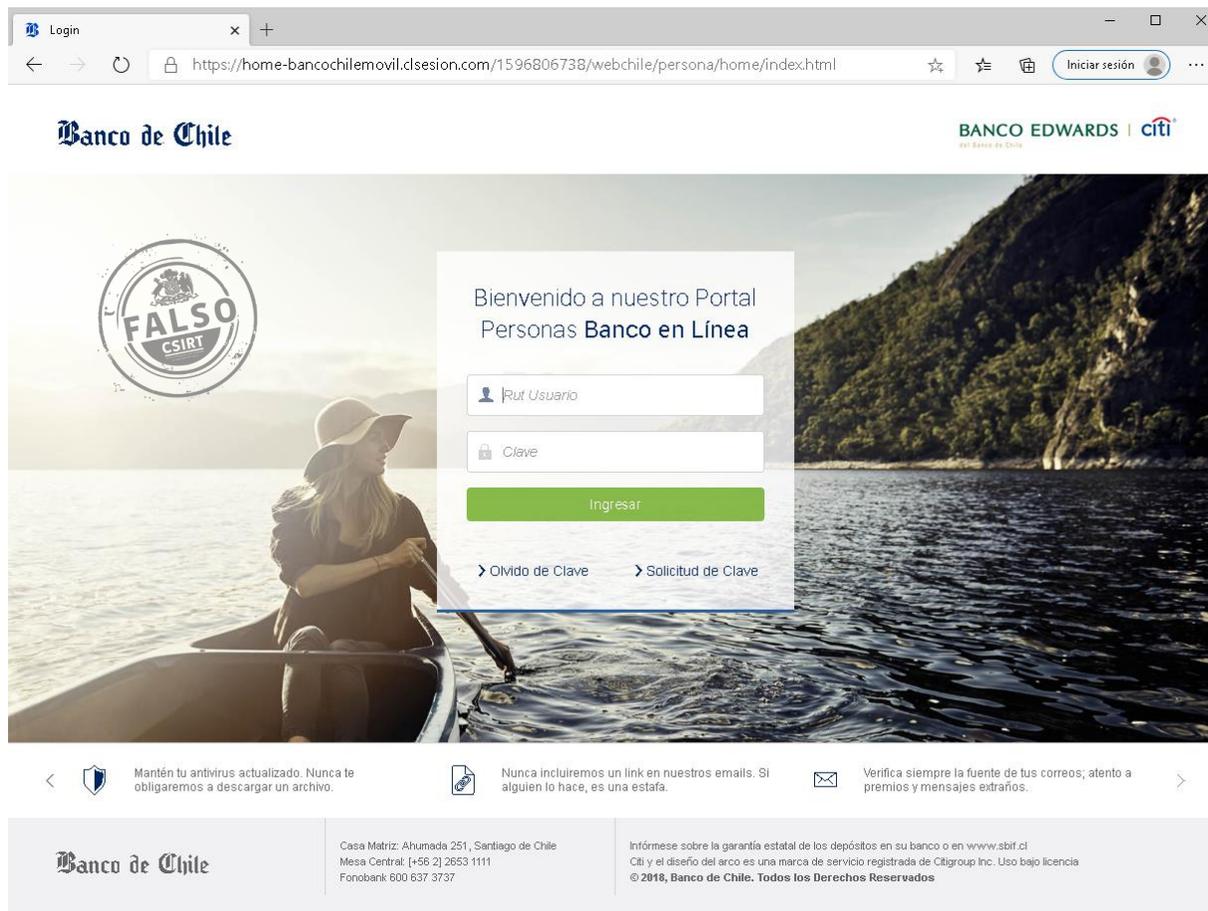
## Datos del Dominio

Nombre de dominio : clsesion[.]com  
Estado del dominio : clientTransferProhibited  
Creado : 2020-08-05  
Expira : 2021-08-05  
Información del registrador : DYNADOT, LLC  
ID IANA : 472  
Correo electrónico : abuse@dynadot.com  
Servidores de nombres : ns1.clsesion.com  
ns2.clsesion.com

BancoChile - Se ha registrado con éxito tu solicitud de retiro máximo del 10 % de AFP. Consulte saldo y movimientos ahora: <https://info-afp.netpersonascl.com>



## Magen del sitio



The screenshot shows the login page of Banco de Chile. The browser address bar displays the URL: <https://home-bancochilemovil.clesion.com/1596806738/webchile/persona/home/index.html>. The page features the Banco de Chile logo and the 'BANCO EDWARDS | citi' logo. The main content area has a background image of a person in a boat on a lake. A white login form is centered, with a 'FALSO CSIRT' stamp overlaid on it. The form contains the following elements:

- Text: "Bienvenido a nuestro Portal Personas Banco en Línea"
- Input field: "Rut Usuario"
- Input field: "Clave"
- Green button: "Ingresar"
- Links: "Olvido de Clave" and "Solicitud de Clave"

At the bottom of the page, there are three security notices:

- 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 fuente de tus correos; atento a premios y mensajes extraños.

The footer contains the Banco de Chile logo, contact information (Casa Matriz: Ahumada 251, Santiago de Chile; Mesa Central: (+56 2) 2653 1111; Fonobank 600 637 3737), and a disclaimer: "Infórmese sobre la garantía estatal de los depósitos en su banco o en [www.sbf.cl](http://www.sbf.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.