

Alerta de seguridad informática	8FPH22-00500-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de marzo de 2022
Última revisión	31 de marzo de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones propias del CSIRT de Gobierno. La información contenida en los informes o comunicados está afectada 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 de Gobierno) ha identificado una campaña de phishing vía correo electrónico que proviene, supuestamente, del Banco Chile. En esta campaña, los delincuentes indican falsamente a la víctima que existe un aumento de cupo en la tarjeta pre aprobado online el cupo y que puede revisar en un enlace disponible en el correo. Al seleccionarlo, la persona es dirigida a un sitio falso, semejante al Banco Chile, donde se expone al robo de su usuario y contraseña (credenciales).

Observación

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

Indicadores de compromiso

Urls redirección:

[https://bit\[.\]ly/portal_consumo](https://bit[.]ly/portal_consumo)
[https://parasolbook\[.\]com/chile.php](https://parasolbook[.]com/chile.php)
[https://xcl-persona\[.\]nl/](https://xcl-persona[.]nl/)

Urls sitio falso:

[https://personas-chile\[.\]cf/1648732150/bchile-web/persona/login/index.html/login](https://personas-chile[.]cf/1648732150/bchile-web/persona/login/index.html/login)

Asunto:

Aumenta online el cupo de tu Tarjeta y/o Línea de Crédito

Correo de salida:

[a1.cl_vl50sf3ihhc@a1\[.\]cl](mailto:a1.cl_vl50sf3ihhc@a1[.]cl)

SMTP Host:

[15.235.59.112]

Otros antecedentes

Certificado Digital

Fecha Valido	:	31-03-2022
Fecha Término	:	29-06-2022
Emitido	:	Let's Encrypt R3

Datos Alojamiento y Dominio

IP	:	[91.209.70.109]
Número de sistema autónomo (AS)	:	43317
Etiqueta del sistema autónomo	:	FNK LLC
País	:	RU
Registrador	:	EU
Información del registrador	:	

Imagen del mensaje

Aumenta online el cupo de tu Tarjeta y/o Línea de Crédito



Consulta si tienes pre aprobado un aumento de cupo



REVISA AQUÍ

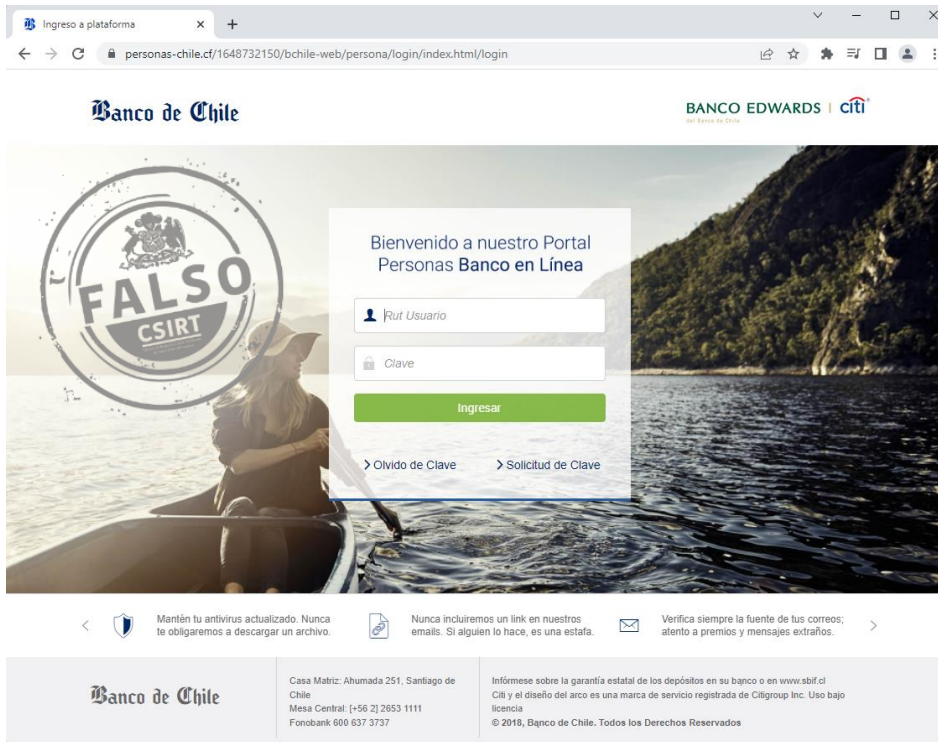
VIGENCIA

Vigencia desde el 1 al 31 de marzo de 2022.

Vigencia desde el 1 al 31 de marzo de 2022. Otorgamiento de aumento de cupo de Línea de Crédito y/o Tarjeta de Crédito señalado sujeto a que se mantengan condiciones comerciales y financiera del cliente consideradas al momento de la evaluación.

Casa Matriz: Ahumada 251, Santiago de Chile
Infórmese sobre la garantía estatal de los depósitos en su banco o en www.sbf.cl
2022 Banco de Chile. Todos los Derechos Reservados.

Imagen del sitio



The screenshot shows a web browser window with the URL `personas-chile.cf/1648732150/bchile-web/persona/login/index.html/login`. The page header features the **Banco de Chile** logo on the left and **BANCO EDWARDS | citi** on the right. The main content area is a login portal titled "Bienvenido a nuestro Portal Personas Banco en Línea". It includes a large circular watermark that says "FALSO CSIRT" overlaid on a background image of a person in a boat on a lake. The login form contains fields for "Rut Usuario" and "Clave", an "Ingresar" button, and links for "Olvido de Clave" and "Solicitud de Clave". Below the form, 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.", and "Verifica siempre la fuente de tus correos; atento a premios y mensajes extraños." The footer contains the Banco de Chile logo, contact information for the Casa Matriz (Ahumada 251, Santiago de Chile) and Mesa Central (+56 2) 2653 1111, Fonobank 600 637 3737, and a disclaimer about the state guarantee of deposits and the use of the Citigroup logo.

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.