

Alerta de seguridad cibernética	8FFR22-01078-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de abril de 2022
Última revisión	26 de abril de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia 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 fraude 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 fraude, 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 del Gobierno de Chile (CSIRT de Gobierno) ha identificado la activación de una página fraudulenta que suplanta a la plataforma del Banco de Chile, la que podría servir para robar credenciales de sus usuarios.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad aludida.

Indicadores de compromiso

URL sitio falso

hXXps://portales-personas-bancochirle-cl.portalogin[.]cf/1650986234/bchile-web/persona/login/index.html/login

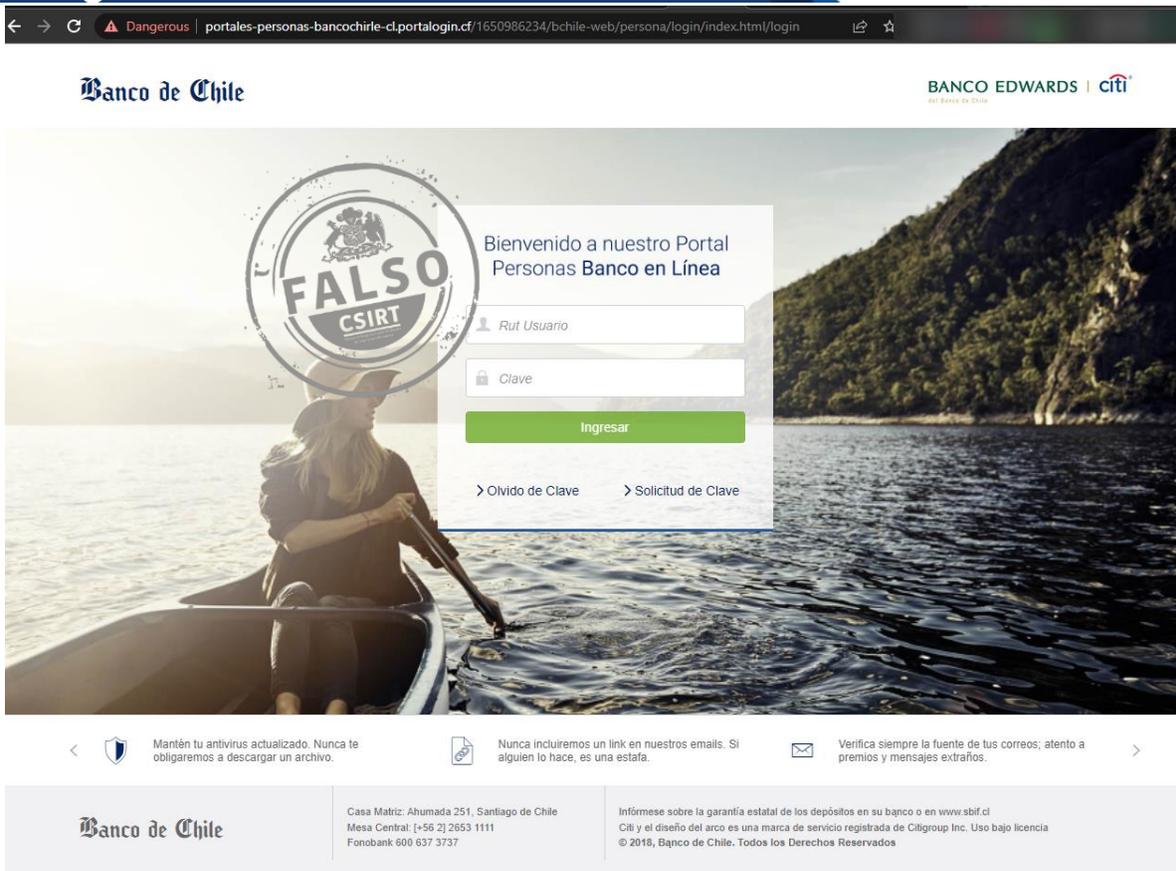
Certificado Digital

Fecha Válido : 26-04-2022
Fecha Término : 25-07-2022
Emitido : Let's Encrypt E1

Datos Alojamiento

IP : [172.67.203.174]
Número de Sistema Autónomo (AS) IP : 13335
Etiqueta del Sistema Autónomo IP : CLOUDFLARENET
Registrador IP : ARIN
País IP : US
Dominio : portalogin[.]cf
Registrador Dominio : NO APLICA

Imagen del sitio



The screenshot shows the login page of Banco de Chile. At the top left is the 'Banco de Chile' logo, and at the top right are the logos for 'BANCO EDWARDS' and 'citi'. The main content area features a background image of a person in a boat on a lake. Overlaid on this is a login form with the heading 'Bienvenido a nuestro Portal Personas Banco en Línea'. The form includes fields for 'Rut Usuario' and 'Clave', an 'Ingresar' button, and links for 'Olvido de Clave' and 'Solicitud de Clave'. A large, semi-transparent watermark with the text 'FALSO CSIRT' is placed over the login form. Below the main content, 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 Casa Matriz, Mesa Central, and Fonobank, and a disclaimer about the state guarantee of deposits and the use of the Citi 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.