

Alerta de seguridad cibernética	8FFR21-01004-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de agosto de 2021
Última revisión	20 de agosto de 2021

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 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 al Banco BCI, 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

[http://139.99.233\[.\]26/1629464710/personas](http://139.99.233[.]26/1629464710/personas)

Certificado Digital

Fecha Válido	No aplica
Fecha Término	No aplica
Emitido	No aplica

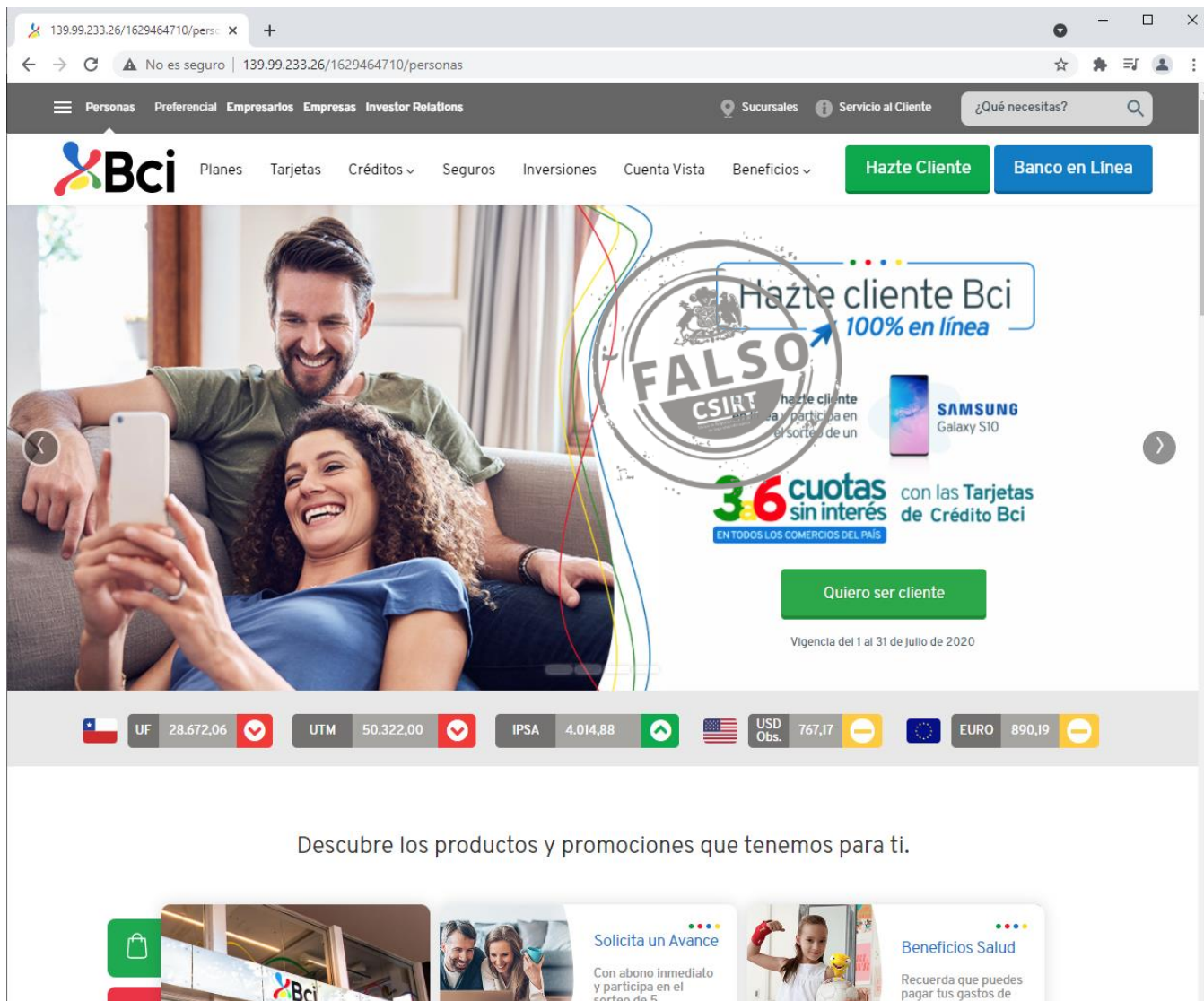
Datos Alojamiento

IP	[139.99.233.26]
Número de Sistema Autónomo (AS)	16276
Etiqueta del Sistema Autónomo	OVH SAS
País	AU
Registrador	APNIC

Datos del Dominio

Nombre de Dominio	No aplica
Creado	No aplica
Expira	No aplica
Información del Registrador	No aplica
ID IANA	No aplica
Correo Electrónico	No aplica
Name Server	No aplica

Imagen del sitio



The screenshot shows the Bci website interface. At the top, there is a navigation bar with links for 'Personas', 'Preferencial', 'Empresarios', 'Empresas', and 'Investor Relations'. A search bar contains the text '¿Qué necesitas?'. Below the navigation bar is the Bci logo and a menu with options: 'Planes', 'Tarjetas', 'Créditos', 'Seguros', 'Inversiones', 'Cuenta Vista', and 'Beneficios'. Two prominent buttons are visible: 'Hazte Cliente' (green) and 'Banco en Línea' (blue).

The main content area features a large image of a smiling couple on a couch. Overlaid on this image is a circular stamp that says 'FALSO' and 'CSIRT'. To the right of the image, there is a promotional banner for 'Hazte cliente Bci 100% en línea'. The banner includes a 'SAMSUNG Galaxy S10' image and text: 'Hazte cliente Bci y participa en el sorteo de un SAMSUNG Galaxy S10'. Below this, it says '36 cuotas sin interés con las Tarjetas de Crédito Bci EN TODOS LOS COMERCIOS DEL PAIS'. A green button labeled 'Quiero ser cliente' is positioned below the banner, with the validity period 'Vigencia del 1 al 31 de Julio de 2020' underneath.

Below the main banner is a currency exchange table with the following data:

Currency	Rate	Change
UF	28.672,06	↓
UTM	50.322,00	↓
IPSA	4.014,88	↑
USD Obs.	767,17	↓
EURO	890,19	↓

Below the table, the text reads: 'Descubre los productos y promociones que tenemos para ti.' Below this text are three promotional cards:

- Solicita un Avance**: Con abono inmediato y participa en el sorteo de 5.
- Beneficios Salud**: Recuerda que puedes pagar tus gastos de...

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.