

Alerta de seguridad cibernética	8FFR20-00705-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de Septiembre de 2020
Última revisión	12 de Septiembre 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 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 (CSIRT), ha identificado la activación de un portal fraudulento asociado a un dominio que suplanta el sitio web oficial de **Banco BCI**, el que podría servir para robar credenciales de usuarios de esa entidad.

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

Indicadores de compromiso

Urls sitio falso:

bci-personas[.]xyz/personas

Body SHA-256

d7ad32a008016a3702d49cdb84ddce0238f8f2a78f5c9d7d9f4bf13dd34b9da7

Certificado Digital

Fecha Valido	:	No Existe
Fecha Termino	:	No Existe
Emitido	:	No Existe

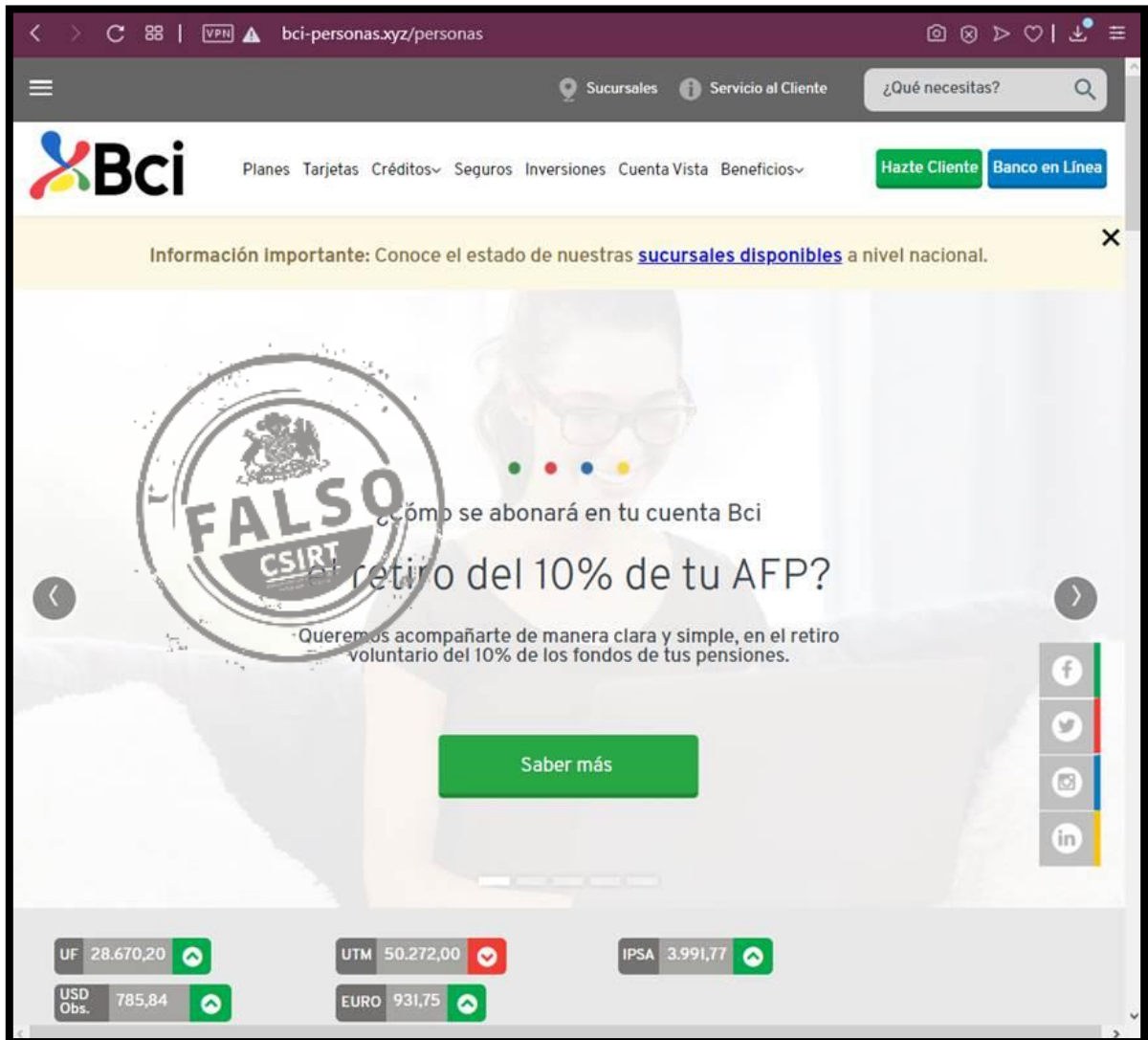
Datos Alojamiento

IP	:	194[.]180[.]224[.]87
Número de sistema autónomo (AS)	:	44685
Etiqueta del sistema autónomo	:	Patron Technology Persia Ltd
País	:	Estados Unidos
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	bci-personas[.]xyz
Estado del dominio	:	Activo
Creado	:	2020-09-11
Expira	:	2021-09-11
Información del registrador	:	NameSilo, LLC
ID IANA	:	1479
Correo electrónico	:	No Registrado
Servidores de nombres	:	v1s1[.]xundns[.]com v1s2[.]xundns[.]com

Imagen del sitio



The screenshot shows a web browser displaying the Bci website. The address bar shows 'bci-personas.xyz/personas'. The website header includes the Bci logo, navigation links (Planes, Tarjetas, Créditos, Seguros, Inversiones, Cuenta Vista, Beneficios), and buttons for 'Hazte Cliente' and 'Banco en Línea'. A search bar is present with the text '¿Qué necesitas?'. A yellow banner at the top reads: 'Información importante: Conoce el estado de nuestras [sucursales disponibles](#) a nivel nacional.' Below this is a large promotional banner for a 10% withdrawal from AFP funds. The banner features a large circular stamp that says 'FALSO CSIRT' and a woman on a phone. The text on the banner asks '¿Cómo se abonará en tu cuenta Bci el retiro del 10% de tu AFP?' and states 'Queremos acompañarte de manera clara y simple, en el retiro voluntario del 10% de los fondos de tus pensiones.' A green 'Saber más' button is centered. Social media icons for Facebook, Twitter, Instagram, and LinkedIn are on the right. At the bottom, there is a financial summary table:

UF	28.670,20	▲
UTM	50.272,00	▼
IPSA	3.991,77	▲
USD Obs.	785,84	▲
EURO	931,75	▲

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.