

Alerta de seguridad cibernética	8FFR20-00702-01
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 Santander**, 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:

personas-bansantander-web[.]cf/pagos-en-linea

### Body SHA-256

a49514f9d832797b490dc85a973cd3853f5239e7d3e4fccf159d1e3ead56767d

### Certificado Digital

Fecha Valido	:	martes, 8 de septiembre de 2020 21:00:00
Fecha Termino	:	martes, 8 de diciembre de 2020 20:59:59
Emitido	:	cPanel, Inc.

### Datos Alojamiento

IP	:	101[.]99[.]90[.]35
Número de sistema autónomo (AS)	:	45839
Etiqueta del sistema autónomo	:	Shinjiru Technology Sdn Bhd
País	:	Malasia
Registrador	:	APNIC

### Datos del Dominio

Nombre de dominio	:	PERSONAS-BANSANTANDER-WEB[.]CF
Estado del dominio	:	Activo
Creado	:	No Registrado
Expira	:	No Registrado
Información del registrador	:	Centrafrique TLD B.V.
ID IANA	:	No Registrado
Correo electrónico	:	No Registrado
Servidores de nombres	:	NS01[.]FREENOM[.]COM NS02[.]FREENOM[.]COM NS03[.]FREENOM[.]COM NS04[.]FREENOM[.]COM

## Imagen del sitio



personas-bansantander-web.cf/pagos-en-linea

#DatoViajero

Santander | Personas | Select | Pymes | Empresas | Private Banking | CIB | Universidades | ? | Beneficios

Cliente | Nuestro Banco | Nuestros Productos | Crédito de Consumo | Tarjetas | Seguros | Inversiones | Mundo Hipotecario

Informate sobre los cursos disponibles, canales de atención digital y medidas de apoyo. AQUÍ

**FALSO CSIRT**

RUT  
Clave  
**Ingresar**  
¿No tienes tu clave?  
Conoce aquí cómo prevenir estafas

**Bienvenido a comprar por internet con tu Tarjeta de Débito Digital.**

Si tienes una tarjeta de débito, bienvenido a comprar por internet. Activa gratis la Tarjeta de Débito Digital aquí.

Paga tus contribuciones en 3 cuotas sin interés. Exclusivo con tus Tarjetas de Crédito Santander.

Beneficios por el planeta. Aprovecha estos descuentos y ayuda al planeta con tus Tarjetas Santander.

Invierte con tranquilidad y confianza. Descubre lo fácil que es invertir aquí.

Lo que debes saber del retiro del 10% de la AFP. Infórmate más aquí.

Seguro Accidentes Urgencias Médicas. Contrátalo online y ob primer mes sin costo. 07 al 20 de septiembre 2020.

Incondicional de La Roja y todas las Rojas

Sanodelucas.cl Educación Financiera

Santander

TECHO CHILE  
40% A LA PUERTA  
WORK/CAFÉ  
SANTANDER CONSUMER

Súmame a #CHILECOMPARTE de TECHO.

Bienvenida Clientes

## 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.