

Alerta de seguridad cibernética	8FPH20-00228-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Mayo de 2020
Última revisión	23 de Mayo 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 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, ha identificado una campaña de Smishing, que se está difundiendo a través de mensaje de texto falso que aparenta provenir del Banco Santander.

La campaña busca persuadir a quienes reciben el mensaje para utilizar el enlace fraudulento adjunto. El mensaje informa que se encuentra aprobado un crédito Covid-19.

Si la persona utiliza el enlace será dirigido a una web fraudulenta que imita al sitio oficial del banco, donde se expondrá al robo de sus credenciales y datos de su tarjeta de crédito.

Observación

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

Indicadores de compromiso

Urls Redirecciones:

hxxps://bit[.]ly/2ZohSLn?l=www.santander.cl

hxxps://www.zouavespontificaux[.]be/activacion/cuenta-feza/

Urls sitio falso:

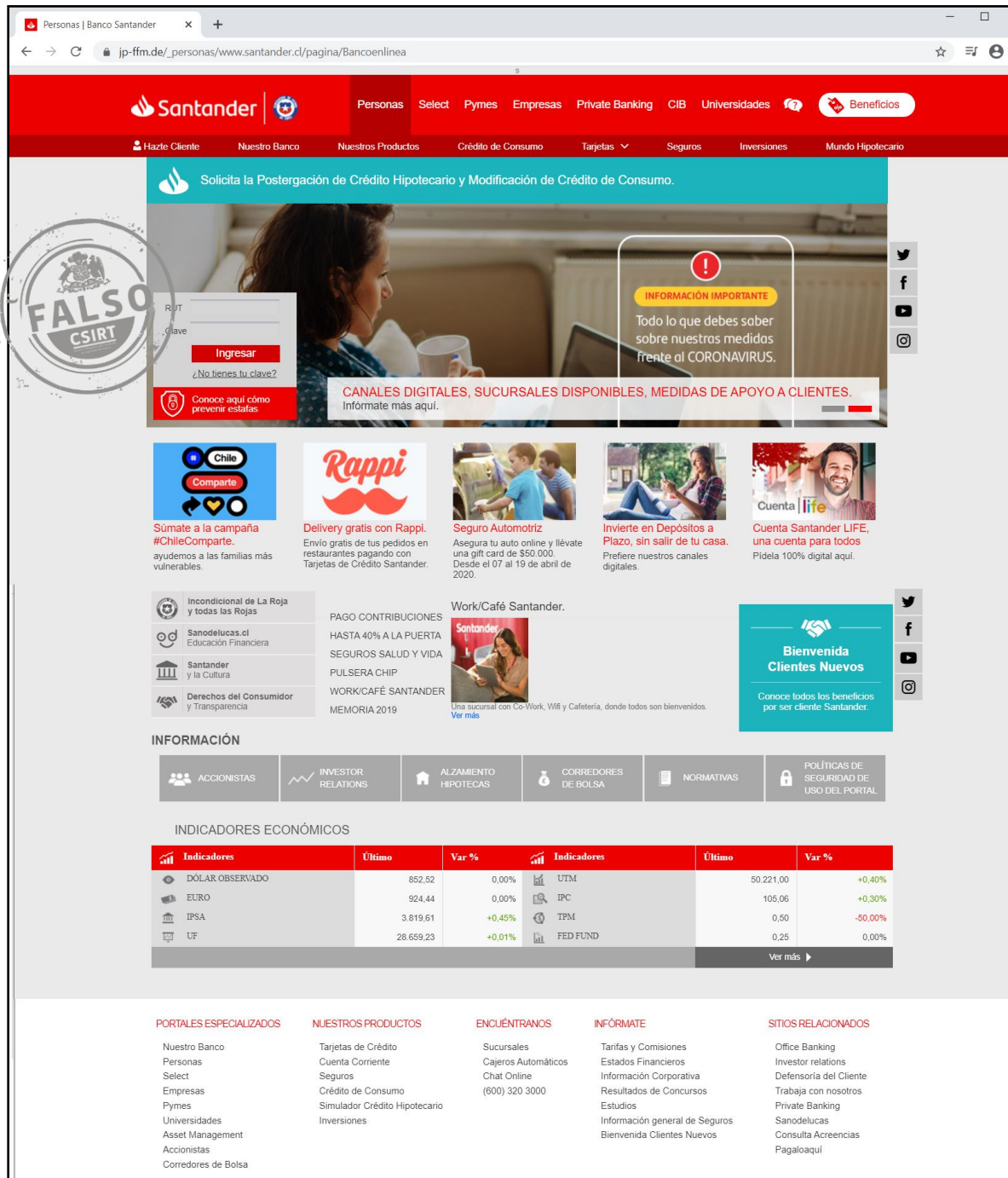
hxxps://jp-ffm[.]de/_personas/www.santander.cl/pagina/Bancoenlinea

Imagen del mensaje

Estimado Cliente Santander. Su
Crédito Covid-19 fue aprobado
ingrese aqui. [https://bit.ly/
2ZohSLn?l=www.santander.cl](https://bit.ly/2ZohSLn?l=www.santander.cl)



Imagen del sitio



Personas | Banco Santander

jp-ffm.de/_personas/www.santander.cl/pagina/Bancoenlinea

Santander

Personas Select Pymes Empresas Private Banking CIB Universidades Beneficios

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

Solicita la Postergación de Crédito Hipotecario y Modificación de Crédito de Consumo.

INFORMACIÓN IMPORTANTE

Todo lo que debes saber sobre nuestras medidas frente al CORONAVIRUS.

CANALES DIGITALES, SUCURSALES DISPONIBLES, MEDIDAS DE APOYO A CLIENTES. Infórmate más aquí.

Sumate a la campaña #ChileComparte

Delivery gratis con Rappi.

Seguro Automotriz

Invierte en Depósitos a Plazo, sin salir de tu casa.

Cuenta Santander LIFE, una cuenta para todos.

Incondicional de La Roja y todas las Rojas

Sanodelucas.cl Educación Financiera

Santander y la Cultura

Derechos del Consumidor y Transparencia

PAGO CONTRIBUCIONES HASTA 40% A LA PUERTA

SEGUROS SALUD Y VIDA

PULSERA CHIP

WORK/CAFÉ SANTANDER

MEMORIA 2019

Work/Café Santander.

Bienvenida Clientes Nuevos

Conoce todos los beneficios por ser cliente Santander.

INFORMACIÓN

ACCIONISTAS INVESTOR RELATIONS ALZAMIENTO HIPOTECAS CORREDORES DE BOLSA NORMATIVAS POLÍTICAS DE SEGURIDAD DE USO DEL PORTAL

INDICADORES ECONÓMICOS

Indicadores	Último	Var %	Indicadores	Último	Var %
DÓLAR OBSERVADO	852,52	0,00%	UTM	50.221,00	+0,40%
EURO	924,44	0,00%	IPC	105,06	+0,30%
IPSA	3.819,61	+0,45%	TPM	0,50	-50,00%
UF	28.659,23	+0,01%	FED FUND	0,25	0,00%

Ver más

PORTALES ESPECIALIZADOS

Nuestro Banco

Personas

Select

Empresas

Pymes

Universidades

Asset Management

Accionistas

Corredores de Bolsa

NUESTROS PRODUCTOS

Tarjetas de Crédito

Cuenta Corriente

Seguros

Crédito de Consumo

Simulador Crédito Hipotecario

Inversiones

ENCUÉTRANOS

Sucursales

Cajeros Automáticos

Chat Online

(600) 320 3000

INFÓRMATE

Tarifas y Comisiones

Estados Financieros

Información Corporativa

Resultados de Concursos

Estudios

Información general de Seguros

Bienvenida Clientes Nuevos

SITIOS RELACIONADOS

Office Banking

Investor relations

Defensoría del Cliente

Trabaja con nosotros

Private Banking

Sanodelucas

Consulta Acreencias

Pagaloaqui

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.