

Alerta de seguridad informática	8FPH22-00601-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de septiembre de 2022
Última revisión	26 de septiembre 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 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 de Gobierno) ha identificado una nueva campaña de phishing vía correo electrónico. En esta campaña, los delincuentes indican falsamente a la víctima lo siguiente: *“Santander, Por motivo de seguridad le informamos que durante la comprobación de nuestra seguridad del presente mes 2022, su cuenta corriente ha sido bloqueada.”* De abrir el archivo, la persona es dirigida a un sitio falso semejante a Banco Santander, donde se expone al robo de su usuario y contraseña (credenciales).

Observación

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

Indicadores de compromiso

URL redirección:

[https://www.skybrands.com\[.\]np/Recuperalo_Aqui/cuenta-sqft/](https://www.skybrands.com[.]np/Recuperalo_Aqui/cuenta-sqft/)

URL sitio falso:

[https://view.cavipando\[.\]xyz/1664198968/portada/personas/home.asp](https://view.cavipando[.]xyz/1664198968/portada/personas/home.asp)

Asunto	Correo de Salida	SMTP Host
✓ FW: Cuenta Bloqueada (VALIDACION DE DATOS)	apache@vmi1015725.contaboserver.net	[62.171.178.173]



Otros antecedentes

Certificado Digital

Fecha Valido	25 Sep 2022
Fecha Término	25 Sep 2025
Emitido	Sectigo Limited

Datos Alojamiento y Dominio

IP	[68.65.122.77]
Número de sistema autónomo (AS) IP	22612
Emitido Etiqueta del sistema autónomo IP	NAMECHEAP-NET
Registrador IP	ARIN
País IP	US
Dominio	cavipando.xyz
Registrador Dominio	namecheap.com

Imagen del }mensaje



SANTANDER BANCO S.A

Estimado Cliente: [REDACTED]

Santander, Por motivo de seguridad le informamos que durante la comprobacion de nuestra seguridad del presente mes 2022, su cuenta corriente ha sido bloqueada.

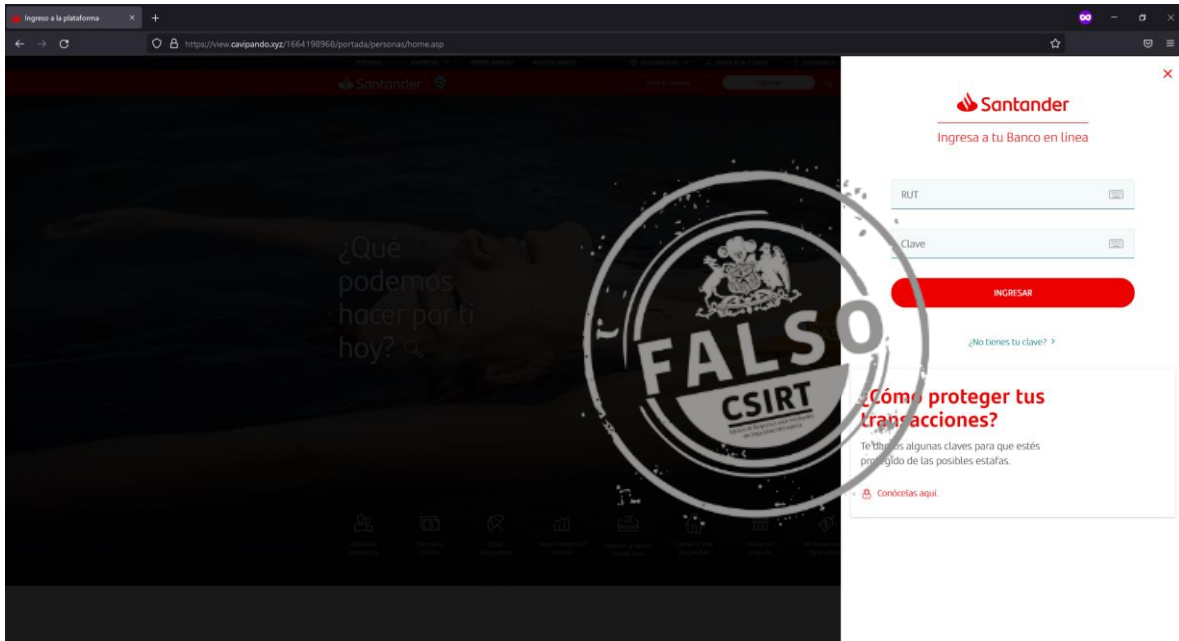
Para evitar que su acceso sea manejada por personas ajenas a usted:



© Banco Santander-Chile, S.A. Todos los derechos reservados.

Informese sobre la garantia estatal de los depositos en su banco o en www.cmfchile.cl / Informese sobre las entidades autorizadas para emitir Tarjetas de Pago en el pais, quienes se encuentran inscritas en los Registros de Emisores de Tarjetas que lleva la CMF, en www.cmfchile.cl / [Políticas de seguridad de uso del portal](#) / Â© 2022 Banco Santander-Chile. Todos los derechos reservados. [Condiciones Objetivas de Contratacion de Productos y Servicios Financieros.](#)

Imagen del sitio



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.

