

| | |
|---------------------------------|---------------------|
| Alerta de seguridad informática | 8FPH21-00351-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 07 de enero de 2021 |
| Última revisión | 07 de enero 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 afectada 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), advierte sobre una campaña de phishing que se está difundiendo, a través de correo electrónico que supuestamente proviene del Banco Santander

El atacante busca persuadir a las personas para utilizar un enlace adjunto.

El mensaje del correo indica que la SúperClave se encuentra bloqueada.

Al seleccionar el enlace para ingresar a activar la SúperClave, es dirigido a un sitio falso, donde se expone al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Urls sitio falso:

[https://www.saantandercl-personas\[.\]com/1610028620/index.asp](https://www.saantandercl-personas[.]com/1610028620/index.asp)

Asunto

Su Súper Clave se encuentra Bloqueada.

Sender

[errorco@ww2.96hosting.com]

Smtip Host:

[108.166.219.79]

Otros antecedentes

URL Body SHA-256

828e4ddb7642d7ac40d5ff6de8bb2f3bf969c1639594d5efa5466e2ea75435af

Certificado Digital

Fecha Válido : 07-01-2021
Fecha Término : 07-04-2021
Emitido : R3

Datos Alojamiento

IP : 139.59.23.73
Número de sistema autónomo (AS) : 14061
Etiqueta del sistema autónomo : DigitalOcean, LLC
País : IN
Registrador : AS

Datos del Dominio

Nombre de dominio : saantandercl-personas[.]com
Creado : 07-01-2020
Expira : 07-01-2022
Información del registrador : Name.com, Inc.
Correo electrónico : abuse@name.com
Servidores de nombres : ns1.dnsowl.com
ns2.dnsowl.com
ns3.dnsowl.com

Imagen del mensaje



Santander


Su Super Clave se encuentra Bloqueada.


Realice el proceso de verificación de lo contrario su servicio de banca por internet quedara temporalmente suspendida.



Su Super Clave se encuentra Bloqueada

Restablecer

 **Descarga nuestra App**
y úsala para lo que necesites.

 
@Santanderchile

Banco Santander-Chile es agente colocador de los diferentes Fondos Mutuos administrados por Santander Asset Management S.A. Administradora General de Fondos. La gestión financiera y el riesgo de estos Fondos Mutuos no guardan relación con la del grupo empresarial al cual pertenecen, ni con la desarrollada por sus agentes colocadores. Infórmese de las características esenciales de la inversión en estos Fondos Mutuos, las que se encuentran contenidas en sus reglamentos internos y folletos informativos. Las rentabilidades o ganancias obtenidas en el pasado por estos Fondos Mutuos no garantizan que ellas se repitan en el futuro. Los valores de las cotas de los fondos mutuos son variables. El riesgo y retorno de las inversiones del Fondo Mutuo Santander GD Acciones USA, así como su estructura de costos, no necesariamente se corresponden con aquellos de los referentes utilizados en la comparación. Infórmese sobre la garantía estatal de los depósitos en su banco o en www.cmfchile.cl.

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.