

Alerta de seguridad informática	8FPH22-00602-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de septiembre de 2022
Última revisión	27 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: *“La SuperClave es una tarjeta de coordenadas que debes llevar contigo cada vez que quieras hacer un movimiento de fondos desde tus productos.”*

De abrir el archivo, la persona es dirigida a un sitio falso semejante a del 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://nam10.safelinks[.]protection.outlook.com/?url=https%3A%2F%2Flinkprotect.cudasvc.com%2Furl%3Fa%3Dhttps%253a%252f%252fmaletashere.com%252fsantander.php%26c%3DE%2C1%2Cpi5x7VmivpdttdPj6sgtXDyflj3-i_pAExn7-PKWLOliwelDpWR8tdgyOb5VRSC_DwABkLxYRSOFI2vguRA2V4xrgfZRxwdTrOR_YRu2H1sVKUcLxUzD8X4%2C%26typo%3D1&data=05%7C01%7Cwaleska.artea%40sea.gob.cl%7C91a54ca86644e8d006408daa001144f%7Cb71dc67ef57148469db81264f14ea88b%7C1%7C0%7C637998224384263779%7CUnknown%7CTWFpbGZsb3d8eyJWljoimC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTiI6Ikh1aWwiLCJXVCI6Mn0%3D%7C1000%7C%7C%7C&sdata=ja%2B1nuxuz7i75ZajkMHjm1pSDvC2qQov0hT5K3ZdfYc%3D&reserved=0
```

[https://maletashere\[.\]com/santander.php](https://maletashere[.]com/santander.php)

URL sitio falso:

[https://bancosantander-cl.netsms\[.\]info/1664285301/portada/personas/home.asp](https://bancosantander-cl.netsms[.]info/1664285301/portada/personas/home.asp)

Asunto	Correo de Salida	SMTP Host
Estado de tu SuperClave requiere Activación	sysuser_7@78.com	[209.222.82.250]

Otros antecedentes

Certificado Digital

Fecha Valido	29 Aug 2022
Fecha Término	27 Nov 2025
Emitido	Let's Encrypt E1

Datos Alojamiento y Dominio

IP	[104.21.69.206]
Número de sistema autónomo (AS) IP	13335
Emitido Etiqueta del sistema autónomo IP	CLOUDFLARENET
Registrador IP	ARIN
País IP	US
Dominio	netsms.info
Registrador Dominio	http://www.namesilo.com

Imagen del mensaje



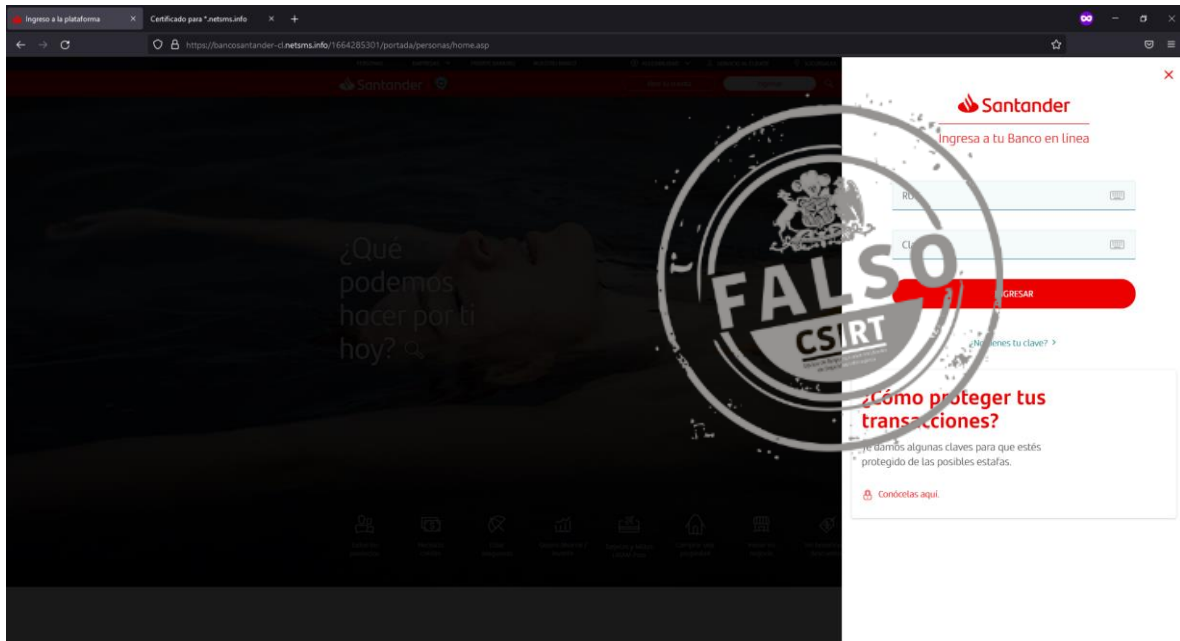
Estado de tu SuperClave requiere Activación

La SuperClave es una tarjeta de coordenadas que debes llevar contigo cada vez que quieras hacer un movimiento de fondos de tus productos.

Úsala de forma segura cuando en cuenta las siguientes consideraciones.

[Restablecer](#)

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.

