

Alerta de seguridad cibernética	8FPH21-00428-01
Clase de alerta	Fraude
Tipo de incidente	smishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de agosto de 2021
Última revisión	20 de agosto 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 IoC 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 IoC 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) advierte sobre una campaña smishing está siendo difundida y que se hace pasar como proveniente del Banco Santander.

El atacante busca que la persona que recibe el mensaje utilice un enlace ubicado en el cuerpo del mensaje de texto. Ese mensaje indica falsamente que existe un intento de ingreso a la cuenta desde un dispositivo, dejando un enlace para que haga clic. Al seleccionar el link, la víctima es dirigida 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

**Texto Mensaje:**

Santander. Hay un intento de ingreso a tu cuenta desde un nuevo dispositivo. Si no eres tu, ingresa ahora [https://santander.viasms\[.\]app/](https://santander.viasms[.]app/)

**URL de SMS:**

[https://santander.viasms\[.\]app/](https://santander.viasms[.]app/)

**URL sitio falso:**

[https://santander.personas-movil\[.\]xyz/1629462954/personas/index.asp](https://santander.personas-movil[.]xyz/1629462954/personas/index.asp)

## Otros antecedentes

### Certificado Digital

Fecha Valido : 14/08/2021  
Fecha Termino : 15/08/2022  
Emitido : Sectigo RSA Domain Validation Secure Server CA

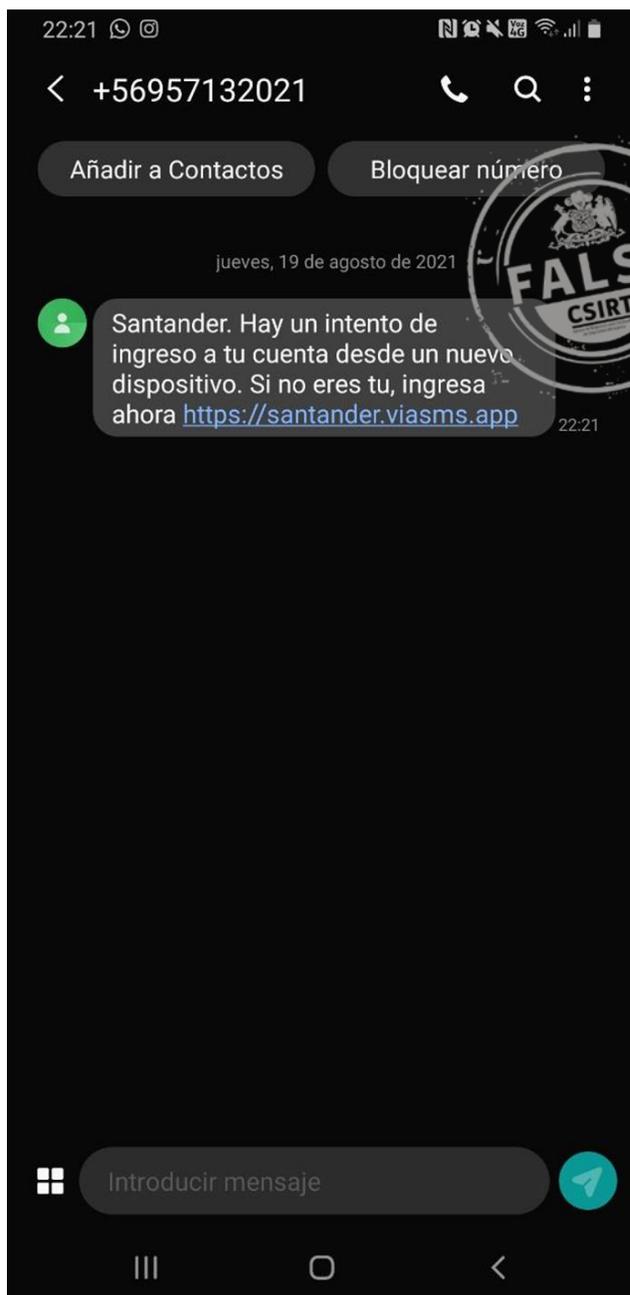
### Datos Alojamiento

IP : [162.0.217.19]  
Número de sistema autónomo (AS) : 22612  
Etiqueta del sistema autónomo : NAMECHEAP-NET  
País : US  
Registrador : ARIN

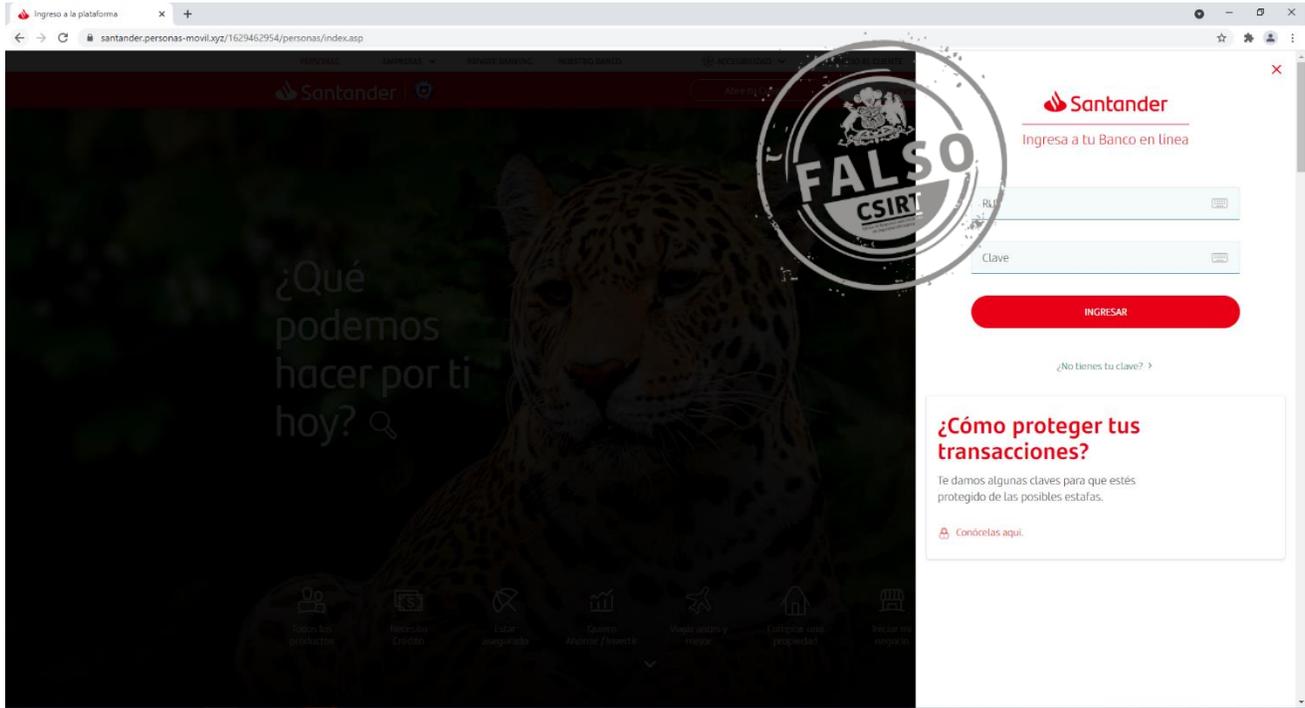
### Datos del Dominio

Nombre de dominio : personas-movil[.]xyz  
Creado : 15-08-2021  
Expira : 15-08-2022  
Información del registrador : Namecheap Inc.  
ID IANA : 1068  
Correo electrónico : abuse@namecheap.com  
Servidores de nombres : dns1.namecheaphosting.com  
dns2.namecheaphosting.com

## Imagen del mensaje



## 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.