

Alerta de seguridad informática	8FPH20-00328-01
Clase de alerta	Fraude
Tipo de incidente	Smishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Noviembre de 2020
Última revisión	16 de Noviembre 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 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 Smishing que supuestamente proviene del Banco Santander.

El atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del mensaje. El mensaje indica que por motivos de seguridad fue bloqueada la tarjeta del cliente, para lo cual solicita verificar la cuenta para reactivar acceso. Con ese fin se dispone de un enlace.

Al seleccionar el enlace para desbloquear la cuenta, la persona 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

### Urls Redirección:

[https://santa-verifigcl\[.\]site/?sms=santander](https://santa-verifigcl[.]site/?sms=santander)

### Urls sitio falso:

[https://smsapp-santacl\[.\]xyz/1605529755/personas/index.asp](https://smsapp-santacl[.]xyz/1605529755/personas/index.asp)

### Mensaje

SANTANDER: Por motivos de seguridad bloqueamos tu Tarjeta de Crédito. Verifica tu cuenta para activar acceso:

## Otros antecedentes

### URL Body SHA-256

dd6a55eeceaf20ef631862bec76f8ca6f3ce42a81a6517ab7072c9c1d5ac9f53

### Certificado Digital

Fecha Valido : 18/10/2020  
Fecha Término : 16/01/2021  
Emitido : Let's Encrypt Authority X3

### Datos Alojamiento

IP : 162.0.235.141  
úmero de sistema autónomo (AS) : 35893  
Etiqueta del sistema autónomo : AirComPlus Inc  
País : CA  
Registrador : ARIN

### Datos del Dominio

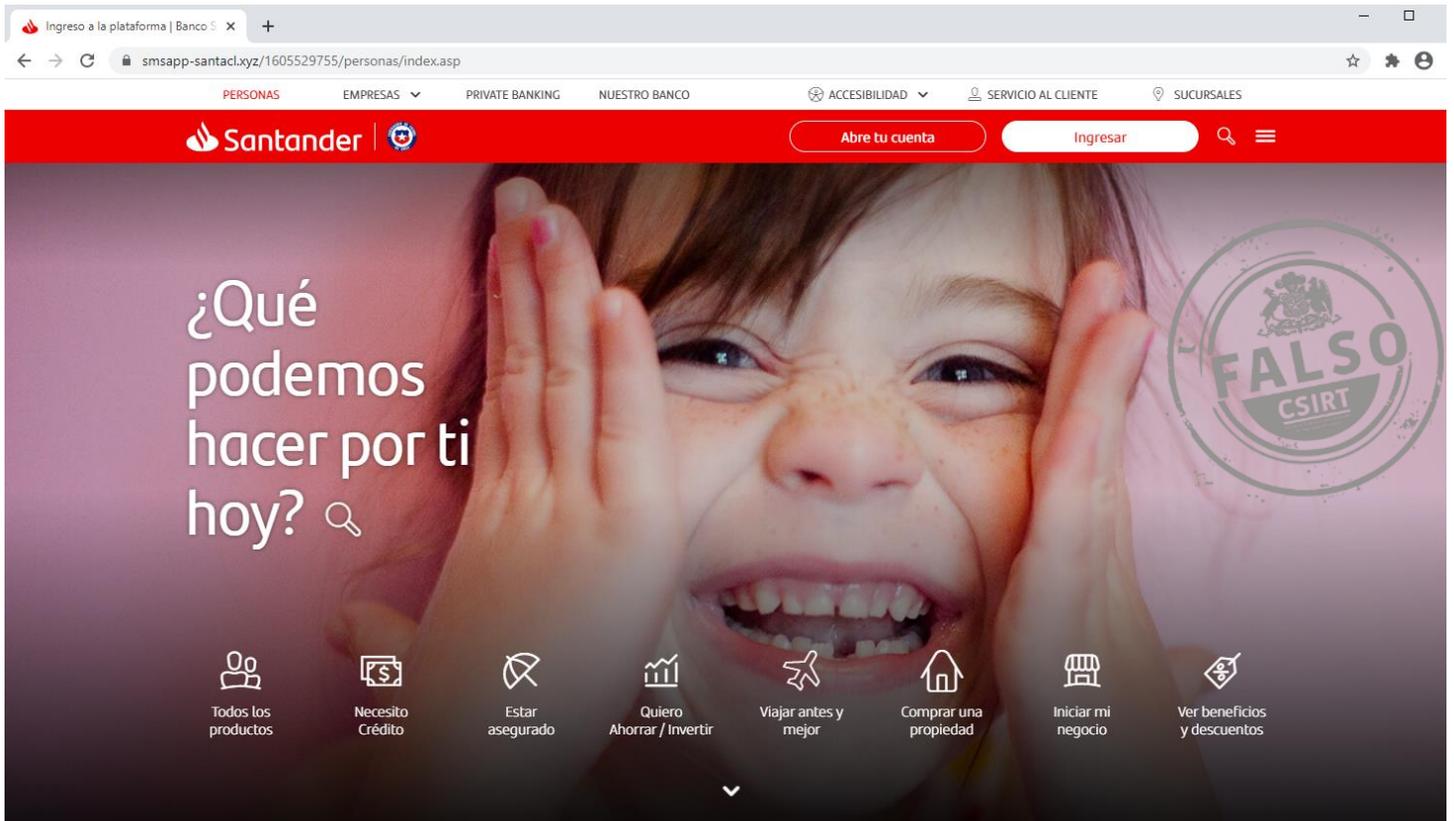
Nombre de dominio : verifigcl[.]site  
Creado : 14-11-2020  
Expira : 14-11-2021  
Información del registrador : Namecheap  
ID IANA : 1068  
Correo electrónico : abuse@namecheap.com  
Servidores de nombres : dns1.namecheaphosting.com  
dns2.namecheaphosting.com

## Imagen del mensaje

SANTANDER: Por motivos de seguridad bloqueamos tu Tarjeta de Credito. Verifica tu cuenta para activar acceso:  
<https://santa-verifigcl.site/?sms=santander>



## 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.