

Alerta de seguridad informática	8FPH21-00377-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Febrero de 2021
Última revisión	23 de Febrero 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) del Gobierno de Chile, advierte sobre una campaña de phishing que está siendo difundida a través de correo electrónico y que supuestamente proviene del Banco Santander

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

El mensaje del correo indica que el banco realizaron un monitoreo de las actividades de la cuenta y por ese motivo fue bloqueada y debe realizar el proceso de verificación. Al seleccionar el enlace para realizar la activación, se 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 Redirección:

<https://bit.ly/37AZcva?l=www.santander.cl>

<http://wordpress.roma.it/favicon/enviar02.php?l=2010228726>

<http://www.lacreatura.esivalladolid.com/activacion/cuenta-eaqr/>

### Urls sitio falso:

<http://gaborestarsa2005.hu/wp-includes/www.santander.cl/pagina/login.asp>

### Asunto

Notificacion - SuperClave Bloqueada.

SuperClave Bloqueada.

Aviso SuperClave Bloqueada.

### Smtip Sender:

webmaster@example.com

antimonyworldwid@server.designsengine.com

### Smtip Host:

[server.designsengine.com]

[93.125.75.16]

## Otros antecedentes

### Certificado Digital

Fecha Válida : No aplica  
Fecha Término : No aplica  
Emitido : No aplica

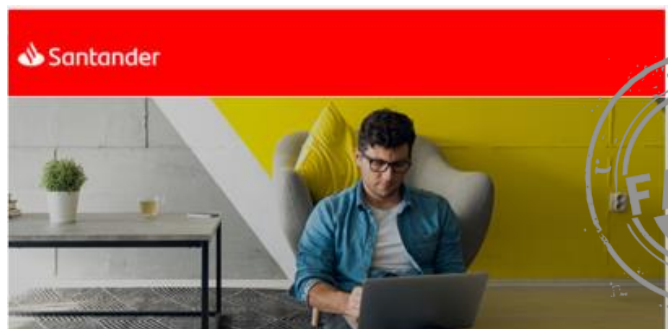
### Datos Alojamiento

IP : 185.6.139.216  
Número de sistema autónomo (AS) : 43711  
Etiqueta del sistema autónomo : Szervernet Ltd  
País : HU  
Registrador : RIPE NCC

### Datos del Dominio

Nombre de dominio : gaborestarsa2005[.]hu  
Creado : 25-03-2009  
Expira : 26-02-2020  
Información del registrador : Gábor és Társa 2005 Kft.  
ID IANA :  
Correo electrónico :  
Servidores de nombres : ns10.brill-life.hu  
ns09.brill-life.hu

## Imagen del mensaje



Estimado(a) Cliente : :

### Santander sigue dedicado a ofrecerte el mejor servicio.

Durante la emergencia de salud que estamos viviendo como país, los bancos al igual que las farmacias, hospitales y supermercados - debemos permanecer en funcionamiento.

Para Banco Santander tu seguridad sí importa, le informamos que realizamos los monitoreos de las actividad de nuestras cuentas, según la nueva ley Nro 20.009, nos hemos puesto en contacto con usted para informarle que su **Cuenta ha sido BLOQUEADA**.

Por no realizar el proceso de verificación, su servicio de banca por internet quedará temporalmente **Bloqueada**.



**Activa tu SuperClave  
aquí**

Atentamente, Santander



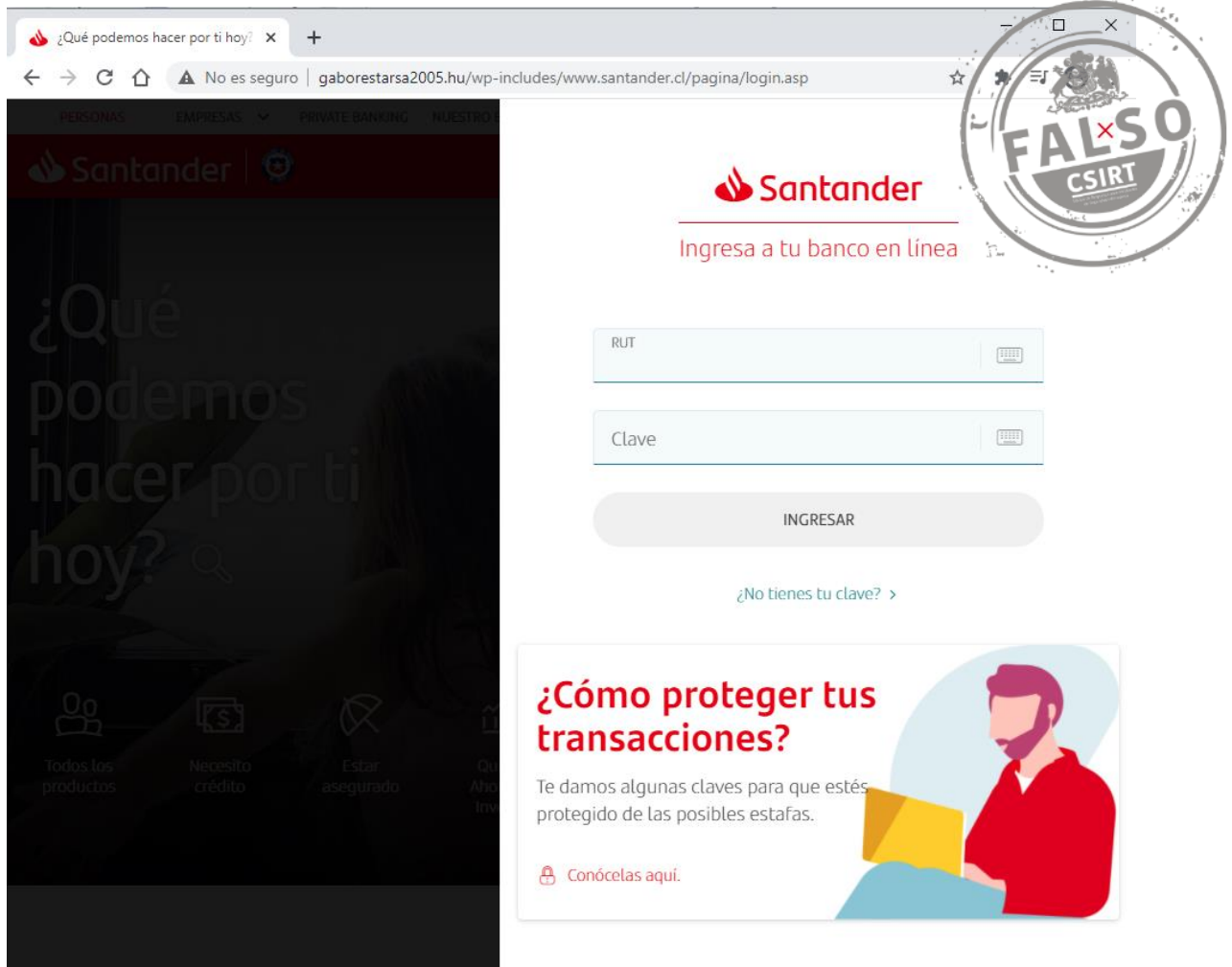
#### TIPS PARA EVITAR ESTAFAS:

- **Nunca, jamás**, te llamaremos para pedir tus claves bancarias o tus coordenadas, ni las pediremos por e-mail ni por SMS.
- **Nunca, jamás**, incluiremos links en nuestros correos electrónicos ni en nuestros SMS.
- **Nunca, jamás**, descargues archivos adjuntos de remitentes desconocidos.



@Santanderchile

## Imagen del sitio



The image shows a screenshot of a web browser displaying the Santander Chile login page. The browser's address bar shows the URL: `gaborestarsa2005.hu/wp-includes/www.santander.cl/pagina/login.asp`. The page features the Santander logo and the text "Ingresa a tu banco en línea". There are input fields for "RUT" and "Clave", followed by an "INGRESAR" button. A link for "¿No tienes tu clave? >" is also present. A large, circular stamp with the word "FALSO" and the CSIRT logo is overlaid on the right side of the page. Below the login form, there is a promotional banner titled "¿Cómo proteger tus transacciones?" with an illustration of a man using a laptop. The banner text reads: "Te damos algunas claves para que estés protegido de las posibles estafas. Conócelas aquí."

## 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.