

www.gruposantander.ru, www.gruposantander.cx y www.gruposantander.tk webs que simulan al Grupo Santander. (ACTUALIZADO)

Empezamos el mes con un ataque phishing a gran escala que puede afectar a clientes del banco Grupo Santander.

Afortunadamente la entidad bancaria Grupo Santander esta realizando todas las gestiones para su cierre inmediato.



Les recordamos que este tipo de engaño o ingeniería social se produce en la mayoría de los casos por medio de la recepción de un correo electrónico y bajo algún tipo de excusa falsa, de esta manera la victima pincha sobre un enlace o rellena un formulario con sus datos.

Las web falsas detectadas por ahora son;

www.gruposantander.cx
www.gruposantander.ru

ACTUALIZADO:
www.gruposantander.tk

Los internautas pueden recibir el siguiente correo electrónico falso, donde nos ruegan que verifiquemos nuestros datos.

RECUERDEN, NUNCA LO TIENE QUE HACER.



Estimados clientes,

Hace unos días en la red de ordenadores de nuestro banco tuvo ocurrencia una desviación técnica.

Algunos clientes no pudieron usar su cuenta.

Le rogamos confirmar sus datos para el acceso on-line.

[Para eso empuje esta referencia y entre en su cuenta.](#)

Gracias por ser Cliente de BSCH.

[Banco Santander Central Hispano, S.A., 2006.](#)
Todos los derechos reservados.

Si una persona victima del engaño pulsa sobre el enlace, le enviará a una web fraudulenta que simula la imagen de la entidad, pueden comprobarlo en la siguiente imagen:




Acceso para Particulares

Puede introducir sus datos de identificación por el sistema tradicional o utilizando el teclado virtual. [Ver Ayuda](#)

1. NIF

2. Clave de Acceso

3. Firma Electronica

 [Seguridad](#)

[¿Ha olvidado su clave?](#)



Contraste: alto bajo

Por ahora se detectaron las siguientes web falsas:

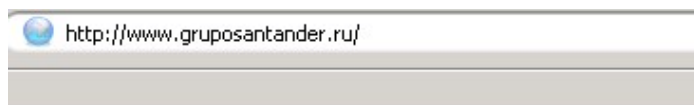
www.gruposantander.cx
www.gruposantander.ru

ACTUALIZADO:

www.gruposantander.tk

Aunque pueden que aparezcan nuevas, por ello no podemos bajar al guardia.

Una vez tecleados nuestros datos en la web falsa nos sale el siguiente mensaje:



Servicio temporalmente indisponible

[Back](#)

Consejos si usted fue victima de este tipo de engaño:

- 1.- Actué rápido.**
- 2.- Cambien las claves privadas por unas nuevas.**
- 3.- Notifique lo antes posible la incidencia a su entidad, no espere a mañana llame de inmediato, las entidades bancarias actuaran al instante sobre este tipo de estafas.**
- 4.- Denuncie el fraude a las Fuerzas de Seguridad del Estado.**

Afortunadamente la entidad inicio las gestiones, para cerrar las páginas con la máxima celeridad.

Desde la Asociación de Internautas repetimos de nuevo que nunca deben de NO CONTESTAR A ESTE TIPO DE CORREOS NI PULSAR LOS ENLACES QUE CONTIENEN ESTE TIPO DE CORREOS ELECTRÓNICOS y lo mas importante su banco NUNCA le solicitara ningún tipo de datos privado como sus claves. Recuerden ellos tienen sus claves y su dinero, en tal caso es usted el que debe de solicitarlas en caso de olvidarlas o extraviarlas.

Aviso de seguridad de Banco Grupo Santander;

Recientemente han sido detectados **emails fraudulentos** enviados a clientes de diferentes Entidades Financieras, solicitando sus datos o claves de acceso a Banca Electrónica. Para evitar ser víctima de un fraude: nunca atienda solicitudes de claves que le lleguen a través de correo electrónico ([amplíe información](#)).

Si tiene dudas llame a **Superlínea: 902 24 24 24**

Medios de comunicación se hacen eco y alertan a los usuarios del grave peligro del phishing y del scam en nuestro país.

[Tele Madrid](#)

[TVE 1](#)

[SeguridaPymes.es ofrece el indicador Alert-Phishing para sitios web.](#)

[INFORME SOBRE LA BANCA ONLINE ¿ES SEGURA? ¿La banca online es vulnerable?](#)

Faq de ayuda sobre phishing;

<http://seguridad.internautas.org/html/1/451.html>

<http://www.seguridadpymes.com/noticia.php?id=5>

La Asociación de Internautas cuenta con un servicio operativo desde hace meses para todos aquellos internautas que quieran reportar información sobre este tipo de fraudes realizados por medio de Phishing, con solo mandar un correo y adjuntar la información a; phishing@internautas.org

Se estudia el caso y se comunica a las Fuerzas de Seguridad del Estado para cursar la denuncia junto a un comunicado de aviso a la entidad suplantada.

- CONSEJOS DE SEGURIDAD -

[Normas de Seguridad para acceder a la banca por internet](#)

[Normas de Seguridad para una clave perfecta en Internet](#)

[Programa que te ayuda a Generar Claves Seguras.](#)

Agradecemos a todos los amigos internautas que participan en la campaña Anti-Phising y denunciaron este tipo de fraudes.

[SeguridaPymes.es ofrece el indicador Alert-Phishing para sitios web.](#)

-----PHISING HISPANO-----

INFORME : [BBVA la entidad más atacada por Phising en 2005.](#)

[SEGUIMIENTO EN LÍNEA](#)

[ALERTA - PHISING](#)

[RECOMENDACIONES](#)

[Normas de Seguridad para acceder a la banca por internet](#)

[Normas de Seguridad para una clave perfecta en Internet](#)

[Programa que te ayuda a Generar Claves Seguras.](#)

[DENUNCIA PHISING](#)

Fecha artículo: 2006-07-03 18:24:16 - url artículo: <http://www.internautas.org/html/807.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org