

Ataque fraudulento de robo de identidad a clientes del Grupo Santander.

Los ciber-delincuentes están preparando sus ataques para la vuelta de las vacaciones y días festivos navideños de esta manera mañana lunes llenar de correos trampas preparados para el robo de identidad y claves bancarias de los clientes de la banca online, ni en la festividad de los reyes magos hay un paron de ataques.

Era de esperar varios ataques fraudulentos en estas fechas, por desgracia tenemos que alertar una vez mas de un intento de robo de claves bancarias, esta vez **afecta a los clientes del Grupo Santander, afortunadamente la entidad bancaria esta realizando las gestiones necesarias para el cierre inmediato de las web trampas, tras el aviso de la Comisión de Seguridad de la Asociación de Internautas.**

El ataque se produce tras la recepción de un correo trampa que simula ser la entidad bancaria. **RECUERDE ESTE CORREO NO FUE ENVIADO POR SU ENTIDAD BANCARIA, NI NUNCA LE SOLICITARAN ESTOS DATOS POR CORREO ELECTRONICO, ES USTED EN CASO DE PERDIDA.**

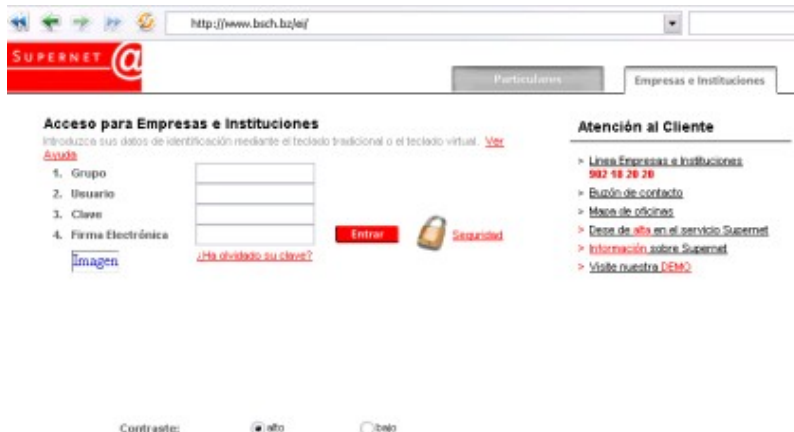
El correo trampa contiene una excusa para que el cliente usuario pulse sobre los enlaces que contiene dicho correo, por ejemplo en este caso es; **ACTIVAR DE NUEVO LAS CUENTAS POR UN CAMBIO DE SEGURIDAD INFORMATICA.**

Correo electrónico trampa recibido:

De: Banco Santander Central Hispano [mailto:inf@santandercentralhispano.es]
Enviado el: domingo, 07 de enero de 2007 19:00
Para: [redacted]
Asunto: Banca Privada



Si se pulsa sobre los enlaces nos puede llevar a distintas web trampas, donde simulan la imagen de la entidad bancaria y la entrada de datos:



Una vez tecleadas las claves nos muestra el siguiente mensaje:

http://www.bsch.bz

Servicio temporalmente indisponible
[Back](#)

Desde la Asociación de Internautas recomendamos que - NO RESPONDAN A ESTE TIPO DE CORREOS , NI PULSEN LOS ENLACES QUE CONTIENEN . Su banco NUNCA le solicitará sus datos privados o sus claves para acceder a su cuenta online.

Los Bancos son depositarios de sus claves y nunca las piden, ni por teléfono, ni por fax ni por correo, ni físicamente es Usted el que debe de solicitarlas en caso de olvidarlas o extraviarlas.

Consejos si usted fue víctima 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.

Aviso de seguridad del 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**

CASOS Y RECOMENDACIONES SOBRE EL PHISHING

[Guía rápida para reconocer páginas web falsas que simulan entidades bancarias.](#)

[Guía rápida para conocer los nuevos fraudes que se producen en la red.](#)

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

[Se abre el debate: ¿Podemos prevenir posibles ataques de fraude de phishing bancario?.](#)

[Internautas Televisión: Informe phishing 2006 en España.](#)

[Internautas Televisión: ROBOS DE CLAVES.](#)

[Internautas Televisión: Phishing.](#)

[Internautas Televisión: ¿Cuánto cuesta un ataque phishing?](#)

[Internautas Televisión: Guía de fraudes en la red.](#)

-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](#)

[LE PUEDE PASAR A CUALQUIERA.](#)

[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.es/noticia.php?id=5>

La Asociación de Internautas cuenta con un servicio operativo desde diciembre de 2004, a disposición de todos aquellos internautas que quieran reportar información sobre este tipo de fraudes Phishing, pueden 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.

- CONFIANZA EN LÍNEA-

[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.](#)

-----SEGUIMIENTO DEL PHISHING EN ESPAÑA DESDE 2004-----

INFORME 2006: [El Phishing en España se incrementa un 290% en 2006.](#)

INFORME 2005: [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 PHISHING](#)

Fecha artículo: 2007-01-07 19:43:45 - url artículo: <http://www.internautas.org/html/1010.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