

Ejemplo de Mail Fraudulento (Phishing)

Primeros signos de alerta

Dirección que no se corresponde a la entidad



Estimado Cliente,
Tras detectar fallo tecnico en nuestra red informatica, nos gustaria informarle como cliente de nuestra entidad bancaria que estamos instalando un nuevo programa de seguridad para hacer mas fiable y seguras sus operaciones.
Para poder acceder a nuestro nuevo programa de seguridad en todas las operaciones de Banca por Internet, tienes que confirmar sus datos.

[Aceptar](#)

Nuestro objetivo es que usted introduzca sus datos de acceso para La Verificacion Del Sistema. Si la verificación no se realiza dentro de 48 Horas su cuenta sera suspendida temporalmente hasta que su registro se haya completado.
Esto solo le costara unos minutos de su tiempo y tendras una seguridad mucho mas compleja.

Todos los Derechos Reservados 2014© BancoSantander.

Solicitud para ejecutar un programa de seguridad. Esto NUNCA nos lo deben pedir por correo electrónico.

Si pasamos el ratón por el enlace vemos que nos lleva a un sitio ajeno al Banco Santander

https://www.obu.co.il/modules/mod_templateselector/BancoSantander/

En la cabecera completa se puede ver unas direcciones "extrañas" de dominio .br, que en principio parecen ser ajenas al banco Santander

De Santander <santander@sac.net>

Asunto Aviso Seguridad Banco Santander.

A

Message ID <682d83037104b36bd166dc8f5700e2a5@sinpospetro.org.br>

Return-Path <sinpospe@meu.meusitecuidoeu.com.br>

Delivered-To <0610240756@buzon.uma.es>

Received from socrates.sci.uma.es by socrates.sci.uma.es (Dovecot) with LMTP id gUMALfCrSFQPZwAA6w15Eg for <0610240756@buzon.uma.es>; Thu, 23 Oct 2014 09:22:08 +0200

Contacto:



C.S.U.

Centro de Servicio al Usuario

Apoyo Tecnológico a la Docencia y la Investigación - S.C.I.

<http://www.sci.uma.es/cau>

Mail: cau@uma.es

Teléfono: 951953000