

Guía rápida para reconocer páginas web falsas que simulan entidades bancarias.

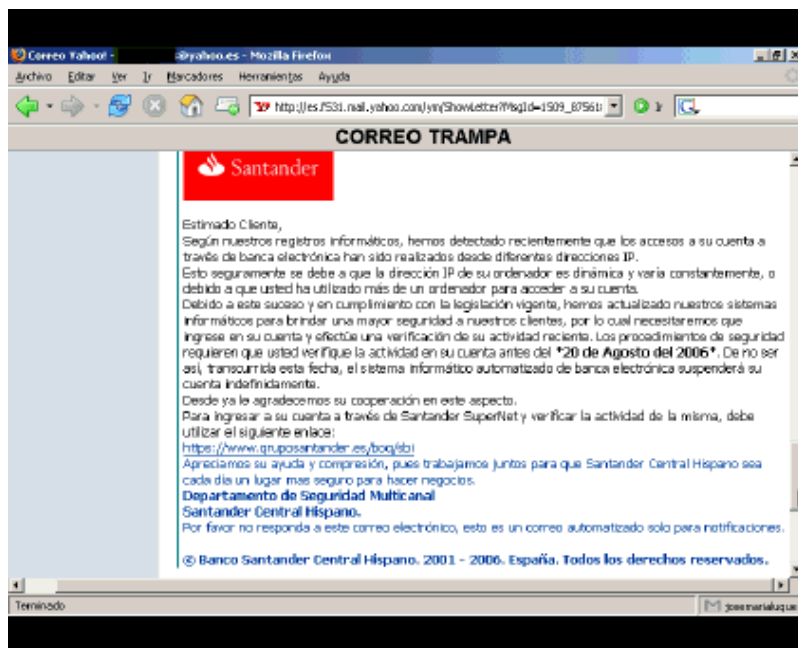
Muchos internautas nos preguntan como reconocer de forma rápida un página web fraudulenta, para agilizar una ayuda rápida y mas en estas fechas que el numero de ataques fraudulentos de casos de phishing bancarios se multiplican. La Comisión de Seguridad de la Asociación de Internautas acaba de realizar dos videos de web reales que están operativos.

Con estos dos ejemplos se quiere enseñar de forma rápida a reconocer los puntos mas importantes a la hora de encontrarnos con una web falsa. También se advertimos que muchos ataques profesionales pueden falsificar algunos consejos que se dan en la guía.

Recuerden son consejos rápidos y facil de recordar, para reconocer una web fraudulenta, recuerde que la mejor prevención es uno mismo y siempre es mejor teclear la dirección del banco y nunca pulsar sobre ningún enlace, además de acordarnos de verificar siempre la certificación de autenticación de la web, pulsando dos veces sobre el candado.

Proceso completo desde la recepción del correo fraudulento.

En el siguiente video se muestra como se produce todo el proceso del engaño desde la recepción del correo trampa donde nos comunican un falso mensaje de seguridad, hasta como llegamos a la web falsa para teclear las claves bancarias. Se puede apreciar que **no estamos bajo una conexión segura ni en ningún momento podemos comprobar la certificación de autenticidad de la web donde nos encontramos.**



[Ampliar vídeo demostrativo.](#)

Ejemplo de web falsa que simula ser Caja Madrid.

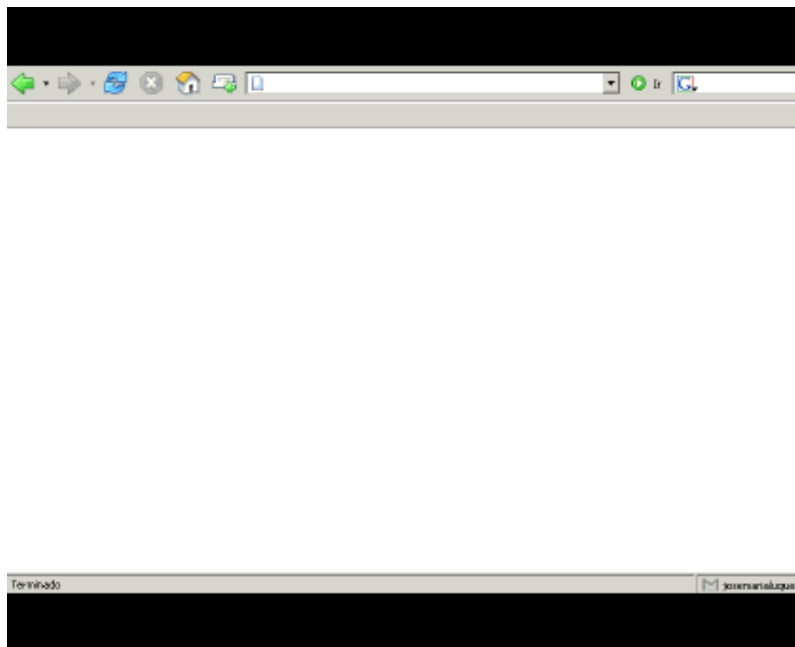
En el siguiente ejemplo se puede comprobar que las imágenes y la forma de la web es idéntica a Caja Madrid pero en ningún momento estamos bajo una conexión segura (**HTTPS://**), **el servidor no es seguro**, ni tampoco vemos por ningún lado el famoso **CANDADO DE SEGURIDAD AMARILLO** para verificar la certificación de autenticidad de la web donde nos encontramos, estos dos puntos son muy importantes, la url es parecida pero no es la real, recuerde que es recomendable siempre teclearla:



[Ampliar vídeo demostrativo.](#)

Web falsa y nombre del dominio que es de Rusia, (ejemplo fraudulento de un ataque al Grupo Santander).

Otro ejemplo similar, pero este aun nos puede llamar la atención al ser tan llamativo y es reconocer el nombre del dominio que **termina en punto RU**, este es lo primero que nos tiene que llamar la atención, el nombre del dominio (URL) es similar pero no el verdadero. No estamos bajo una conexión segura ni vemos por ningún lado el candado de seguridad amarillo:



Esta ayuda rápida para detectar web falsas se complementa con la lectura de la siguiente guía rápida de los nuevos fraudes en la red y las normas básicas para acceder a la banca online , por ultimo como tener un obtener una clave perfecta.

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

[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.](#)

SI QUIERE DENUNCIAR CUALQUIER TIPO DE FRAUDE ONLINE PUEDE REPORTARLO AL SIGUIENTE CORREO ELECTRÓNICO: phishing@internautas.org

Fecha artículo: 2006-08-11 12:19:41 - url artículo: <http://www.internautas.org/html/863.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