

Se abre el debate: ¿Podemos prevenir posibles ataques de fraude de phishing bancario?

La oleada de ataques en el mes de Julio fue constante, la Comisión de Seguridad de la Asociación de Internautas detectó y alertó durante estos 27 días del mes de julio, más de 34 casos de ataques fraudulentos de phishing, sin contar otros tipos de fraudes realizados como ofertas falsas de trabajo (Scam), ni estafas tipo phishing-car.

Muchas veces nos preguntan cómo los usuarios o clientes de las entidades bancarias pueden caer en este tipo de trampa, pero nosotros trasladamos otras preguntas a la entidades bancarias:

¿La entidad bancaria puede prevenir este tipo de ataques?

¿Es culpable la entidad bancaria de estos ataques y qué responsabilidad tiene?

La respuesta a estas preguntas se pueden analizar y contestar desde dos vertientes diferentes y profesionales, aunque estas preguntas pueden generar una gran debate:

Por un lado NO son culpables, es lógico, tanto el cliente víctima de un ataque phishing como la entidad bancaria afectada son afectados por la acción de un ciber-delincuente o estafador.

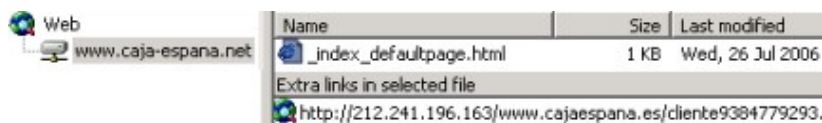
- Al cliente le roban sus claves y su dinero.
- El banco es afectado de forma directa ya que su imagen es dañada por este tipo de ataques.

Por otro lado SI son culpables y vamos a poner un ejemplo claro, la poca prevención ante un posible ataque phishing por parte de alguna entidad bancaria es notable. En la actualidad muchos ataques de phishing se producen por medio de un correo electrónico, éste contiene durante distintos ataques la misma url (dirección) que es usada como **REDIRECCIONADOR** a otras web servidores trampas. La entidad bancaria denuncia y cierra la web trampa, pero dejando en segundo plano la dirección usada como redireccionador en los correos, cuando es esta la responsable del problema. Citamos algunos ejemplos que aun están activos y pueden ser usados para realizar posibles ataques si no se actúa a tiempo:

-Caja España:

<http://www.caja-espana.net/> (ACTIVA, PREVENCIÓN NULA)

Fue usada para un ataque de robo de datos bancarios, aun permanece activa., conducía a la segunda web fraudulenta (está cerrada).



Caja Madrid:

<http://bstadvertising.co.uk/redirect.html> (ACTIVA, PREVENCIÓN NULA)

Fue usada para distintos ataques y puede ser usada para el mismo formato de correo electrónico utilizado en los pasados días.

Las ultimas webs que apuntaba esta dirección/redireccionador fueron las siguientes

*<http://www.age.jp/~azuki/cgi-bin/s3ad/oi.cajamadrid.es>

*<http://pep.co.jp/akc/oi.cajamadrid.es>

En estos ejemplos se puede demostrar que la prevención es nula y pueden llegar a ser responsables de este tipo de fraudes. Los redireccionadores llevan varios días activos,

-¿Que pasaría si hubiera otro nuevo ataque robando datos bancarios a clientes de estas entidades?

-¿Quién sería responsable, el cliente por picar en al trampa?

-¿O sería responsable la entidad por no prevenir a tiempo el posible ataque?

Pasaría como con las víctimas del scam (oferta falsa de trabajo) donde le INGRESAN un dinero en su cuenta procedente de una cuenta bancaria X y la entidad X persigue y denuncia a la víctima como si hubiera sido culpable. Las preguntas están en el aire y **el debate sería muy amplio, con diferentes puntos de vista.**

Para terminar este artículo **el verdadero culpable sería el estafador, creador de una web fraudulenta que suplanta la imagen de una entidad bancaria y envía millones de correos electrónicos falsos para que algún cliente de una entidad caiga en la trampa.** Ya tenemos al verdadero culpable pero eso no le quita responsabilidad a la entidad financiera en temas de prevención. Añadiendo que debe existir información clara y transparente hacia el cliente, sin caer en el actual ocultismo por parte de alguna entidad bancaria, sin olvidar la escasa información por parte de entidades bancarias que deberían informar claramente de los posibles riesgos, con campañas publicitarias iguales o mayores a las de sus productos hipotecarios, préstamos, etc.

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

Si quiere denunciar las estafas que se producen en internet puede usar el siguiente correo electrónico:

phishing@internautas.org

Se estudia el caso y se comunica a las Fuerzas de Seguridad del Estado para cursar la denuncia.

Fecha artículo: 2006-07-27 21:52:03 - url artículo: <http://www.internautas.org/html/836.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