

## Propuestas de la Asociación de Internautas para aumentar la confianza de los clientes bancarios ante el fraude online.

Ante el aumento del fraude online, la Comisión de Seguridad de la Asociación de Internautas en su línea de persecución y acoso contra los ataques Phishing dirigidos a los clientes de las entidades financieras, ha elaborado un informe en el que analiza las posibles soluciones que las entidades financieras debieran adoptar para aumentar la confianza de sus clientes ante este tipo de ataques. Estas propuestas serán puestas a disposición de todas aquellas entidades financieras objeto de suplantación Phishing, interesadas en aumentar la confianza online, el próximo lunes en una reunión de expertos en seguridad informática, auspiciada por el Instituto Nacional de Tecnologías de la Comunicación (INTECO).

Muchos usuarios de la banca online ya conocen las palabras Phishing, troyano, malware, captura teclados, scam, correo trampa, mulero y servidores trampa, todas estas palabras se pueden resumir en una sola **fraude**, ¿Pero se dan soluciones finales al cliente?

Les suena las siguientes palabras, tarjetas de coordenadas, segunda firma, teclado virtual, etc. si, son medidas de seguridad para ser usadas en la banca online, ¿pero esto es la solución a los fraudes online? No, esto es **una medida mas de seguridad incrementada** para que el ciber-delincuente lo tenga mas difícil.

No cabe duda que la **formación y la información** es lo mas adecuado como medida preventiva para poder contrarrestar este tipo de engaños o peligros que puede recibir un cliente de la banca online, pero un cliente que esta en su empresa o en su casa también puede tener otros inconvenientes por muy bien que este formado a la hora de trabaja con la banca online, por ejemplo el ordenador que se utiliza para realizar movimientos bancarios, consultas etc suele ser usado en la mayoría de los casos por mas miembros de la familia o por otros operarios en una oficina, ¿qué peligros con lleva esto? La contestación es muy fácil; muchos peligros, la seguridad de este ordenador ya esta expuesto a la formación de estos nuevo usuarios, sin saberlo la persona encargada de gestionar la banca online puede tener el ordenador infectado con algún capturador de teclas y de imágenes que luego son enviados al ciber-delincuente, como puede ver su maquina ya esta expuesta a gran problema. Otros clientes pensarán que su entidad financiera ya le proporciona unas medidas de seguridad extras como un antivirus actualizable, conjuntamente con un cortafuego para evitar cualquier problema a la hora de trabajar con la banca online, por lo cual se siente tranquilo y baja mas la guardia, desgraciadamente volvemos hablar que tampoco esta a salvó de ser estafado, también puede ser victimas, los troyanos bancarios modernos son capaces de traspasar medidas de seguridad de forma muy fácil, se preguntaran entonces que no hay nada seguro, si reflexiona se dará cuenta que incluso las mejores cajas de seguridad bancarias pueden ser robadas, con esto se contesta todo.

**Ya tengo la solución!!** le pido un ordenador a mi banco para uso exclusivo para operar con la banca online y estaré seguro de los posibles fraudes online, pienso y creo con gran certeza que será bastante difícil que su entidad le de un ordenador a cada cliente de la banca online, por esta misma regla de tres nos debería de dar un coche brindado para llevar nuestros ahorros cuando ingresemos dinero en nuestra entidad.

La verdad que esta difícil dar una solución a los fraudes online, algún cliente pensara al leer este

notas que lo mejor es no ser cliente de la banca online y me ahorro de estos problemas y sustos, pasado unos días a un compañero de trabajo le atracaron al salir del banco cuando llevaba el dinero de las pagos y nominas de la empresa, la moraleja; tampoco fue seguro.

La banca online esta para facilitar muchas operaciones de forma rápida, cómoda y eficaz , puede usar la banca online en cualquier lugar, no tiene que desconfiar de ella, simplemente tiene que conocer los posibles peligros y usar el sentido común, seguro que tiene una gran porcentaje de no ser engañado.

¿Entonces para que me asunta y me meten miedo?, no, en ningún momento se trata de esto, solo transmitía lo que algunos clientes piensa, la pregunta del principio era: **¿Soluciones para los fraudes bancarios online?**

Si existen, pero nunca en seguridad informática se puede hablar del 100%, lo vamos a dejar en un 95% que es un nivel de seguridad muy alto.

Algunas soluciones eficaces:

**Operar con CD-LIVE**, un CD-Live es un sistema operativo que arranca desde un CD, DVD y USB auto-arrancable, este tiene todo lo necesario para poder trabajar con el hardware de su maquina, lo detecta y lo hace operativo para poder trabajar al instante, es casi compatible con la mayoría de las maquinas de empresa y hogares, no tarda mas de 3 minutos en tener operativo una maquina limpia de posibles peligros de troyanos, captura teclados pantalla y a salvo de correos trampa.

La Asociación de Internautas realizó varias pruebas en fase beta el año pasado con distribuciones libres de linux con un resultado muy positivo, en ella cargaba un sistema limpio con un navegador que solo TRABAJA con UNA sola entidad bancaria por motivos de seguridad, se incremenó este punto para que un usuario no buscara la web en cualquier buscador y ser victima de un enlace trampa. Arranca el CD-Live y su escritorio contenía un icono de un navegador que directamente se conectaba con la web de una entidad bancaria.

Este CD-Live contenía las opciones de impresión y guardar documentos de texto en periféricos externos.

Ejemplos de las pruebas de la Asociación de Internautas.



El resultado fue muy exitoso, tampoco importa arrancar con un CD-Live de cada entidad, se incremento en unas de las pruebas un listado de entidades bancarias para no tener que cambiar el CD.

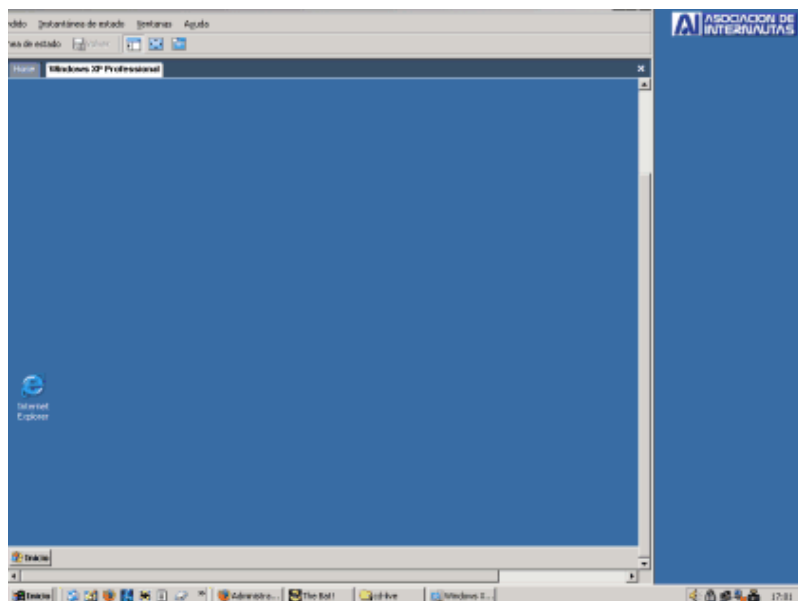
- **Desventajas del CD-Live;** se puede rayar y se debería solicitar otra copia a la entidad. Debería de llevar una marca de agua o similar para identificar a cada cliente.

- **Ventajas del CD-Live;** se puede llevar en cualquier lado, incluso de vacaciones, da igual que sea pirateado no pueden hacer nada con el.

**Nota;** Estos CD-Live beta realizado por la Comisión de Seguridad de la A.I no se pueden distribuir sin el permiso y la supervisión de las entidades bancarias y control numérico de cliente de las entidades.

**Operar con MAQUINA VIRTUAL,** otra opción muy buena, imagen realizada con un sistema operativo que arranca con una maquina virtual, usted tiene un aplicación que llama a un fichero que es donde esta la imagen de un sistema operativo, este contiene lo necesario para poder trabajar, en el se incrementa medidas de seguridad de no instalación, ni escritura del mismo. Es tener dos sistemas operativos ejecutándose a la vez, el normal y el de seguridad bancaria.

Ejemplos de las pruebas realizadas por la Comisión de Seguridad de A.I.



- **Desventaja;** Tienes que tener un programa de maquina virtual, la imagen del sistema trabaja mejor grabada en un HD, no se puede llevar tan fácil a otras maquinas. En un futuro podría existir la posibilidad de capturar paquetes de la maquina principal a la Virtual.

- **Ventajas;** Es muy fácil de usar y cómodo.

Nota; Este tipo maquina virtual se usa bastante en análisis forenses informaticos, para trabajar con una copia de un sistema y obtener pruebas.

**Operar con SMS**, Mensaje corto, sistema utilizado por la entidad bancaria **BANCAJA pionera** en este país en incrementar esta buena medida de seguridad. Consiste en la recepción de un SMS en el móvil con una clave de confirmación para realizar algunas operaciones.

A día de hoy este sistema esta dando unos resultados muy exitoso y con gran aceptación por parte de los clientes. También opera fuera de España.

- **Desventajas;** Es muy caro para una entidad financiera. No esta incrementado en empresas aun, se prevé que en un futuro puedan trabajar con esta iniciativa. Si falla la pasarela contratada de envío SMS tienen que cambiar de forma inmediata.

- **Ventajas;** Este sistema tiene la ventaja de ser muy rápido y genera mucha confianza al cliente.

Después de esta pequeña descripción de posibles soluciones podemos comprobar que a día de hoy si existen soluciones para los fraudes bancarios online.

**Con todo esto no deben de tener miedo a usar Internet, no se asusten estos peligros ya existían antes, no tengan recelo despues de leer este articulo todo al contrario, adaptarse a los nuevos medios tecnológicos es muy importante, pero solo tiene que usar unas pautas de seguridad y sentido común, como el día a día de su vida y no sera victima de estos peligros.**

[Articulo relacionado:](#)

[Kit de phishing, troyanos bancarios y servidores llenos de claves . ¡ Peligro que viene el lobo... ¡.](#)

**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](mailto: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.**

**Comisión de Seguridad en la Red.**

José María Luque Guerrero

<http://seguridad.internautas.org> - [www.seguridadenlared.org](http://www.seguridadenlared.org) - [www.seguridadpymes.es](http://www.seguridadpymes.es)

Asociación de Internautas. [www.internautas.org](http://www.internautas.org)

Fecha artículo: 2007-01-19 18:03:40 - url artículo: <http://www.internautas.org/html/1022.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](mailto:asociacion@internautas.org)