DECÁLOGO DE SEGURIDAD

para acceder a la banca por internet

BANKINTER

www.ebankinter.com

marzo 2005

La banca por Internet es desde hace años una realidad, cada día más personas la utilizan como medio de interactuar y operar con su entidad bancaria.

Sin embargo, miles de personas utilizan diariamente Internet, y no todas tienen intereses lícitos y legales. De manera adicional, el equipo informático que se utiliza para conectarse, navegar y en general operar por Internet, se puede considerar como la extensión "cibernética" del usuario, por lo que su correcto funcionamiento, configuración y seguridad, incidirá directamente en la persona como si de ella misma se tratara.

Como conclusión, no existe más riesgo en el mundo informático en cuanto al dinero, que en el mundo "real", el único problema es el desconocimiento, por lo que tomando las precauciones y hábitos adecuados, podríamos incluso afirmar que comparativamente es más seguro.

A través de este documento, tratamos de proporcionar las guías y normas mínimas de actuación, a través de las cuales poder tomar las precauciones necesarias para conectarse, navegar y operar por Internet.

Normas de Seguridad

1.- Evitar, en la medida de lo posible, acceder a la banca por internet o llevar a cabo transacciones financieras desde lugares públicos, donde el acceso a Internet, es decir, el equipo, la conexión, etc... está disponible para muchas personas. Como hemos indicado en la introducción, el equipo se convierte en la extensión "cibernética" de la persona, por lo que utilizar un equipo del que se desconoce la configuración, software instalado, etc... no es una práctica adecuada.

2.- Mantenga su equipo informático periódicamente actualizado. Disponer de un sistema operativo soportado y actualizable por su fabricante, es un requerimiento necesario en tanto en cuanto cada día se descubren vulnerabilidades en el software que suelen ser explotadas por aquellos internautas con fines delictivos.

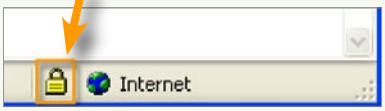
3.- Instale un software antivirus y manténgalo periódicamente actualizado. Disponer de un sistema antivirus es la única herramienta fiable para estar protegido frente a programas y otros software maliciosos. Mantener actualizado este software periódicamente es necesario para que dicha herramienta sea eficaz, teniendo en cuenta que diariamente aparecen nuevos virus frente a los que es necesario estar protegido.

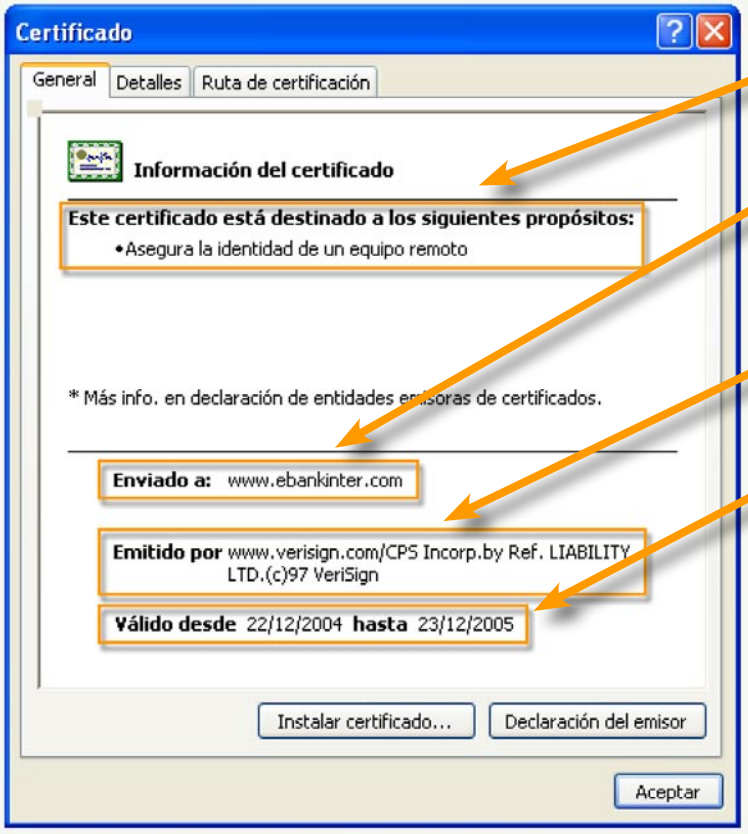
4.- Mantenga su navegador periódicamente actualizado. El navegador es la aplicación a través de la cual se "navega" por Internet. Disponer de una versión actualizada le permitirá disponer de las últimas funcionalidades a nivel de seguridad y estará cubierto frente a vulnerabilidades conocidas que suelen ser explotadas con el objeto de hacerle creer que usted se encuentra conectado a un servidor web distinto del que realmente está.

5.- Conéctese a Bankinter introduciendo manualmente la dirección URL o mediante la utilización de la funcionalidad "favoritos" de su navegador. Acceda al servicio de banca online de Bankinter evitando entrar a través de enlaces ubicados en correos electrónicos y páginas web, a no ser que sean de nuestra entidad. Los enlaces a servicios web pueden ser fácilmente manipulados con el objeto de conectar a otros servicios web que no son los que realmente se muestran en el propio enlace.

6.– Cuando se conecte a los servicio web de Bankinter compruebe que la conexión establecida es segura, es decir, la dirección a la que se ha conectado empieza por https://(•) en vez de http://. A través de una conexión segura no sólo garantiza que toda la información transmitida, en ambos sentidos, viaja cifrada, sino que es la vía para garantizar que usted se está conectando realmente con la banca online de Bankinter.

Un prueba rápida para comprobar la veracidad de la web de nuestro banco, y no ser "estafados" por algunas web diseñadas específicamente para "capturar" datos, es dar "doble clic" sobre el candado amarillo (•) que aparece en la parte inferior derecha de nuestro navegador. Esta acción nos mostrará el certificado de autenticación que asegura, emitido por VeriSign[1], que asegura la identidad de nuestro servicio web.





Comprobaciones a realizar

- La finalidad del certificado debe ser "asegurar la identidad".
- La dirección que aparece en el campo enviado, debe coincidir con la dirección que aparece en el navegador.
- El certificado ha sido emitido por VeriSign[1].
- El certificado es válido, es decir, nos encontramos dentro del periodo de validez del certificado.

Normalmente los navegadores actualizados informan si existe alguna anomalía en el certificado, si bien es recomendable realizar comprobaciones manuales cuando tenga dudas sobre la identidad del servicio web.

[1]**VeriSign** es una Autoridad de Certificación internacionalmente reconocida, algo similar a un notario para servicios Web de Internet.

7.- Proteja sus claves de acceso. Son el medio a través del cual usted se identifica y autentifica frente a nuestros sistemas de Internet, por lo que es necesario que sean personales e intransferibles, es decir, nadie más que usted, debe conocerlas. De manera adicional, existen una serie de consejos de uso común para la elaboración y cuidado de sus claves de acceso:

- No utilice claves que sean fácilmente deducibles por alguien que le conozca.
- Cámbielas periódicamente – dos o tres meses es razonable – y siempre que tenga la menor sospecha de que pueden ser conocidas por alguna otra persona.
- No utilice la funcionalidad de "auto-guardado" de contraseñas disponible en su navegador, ya que implica no tener que teclear sus claves de acceso cada vez que se conecte, y esto puede facilitar que puedan detectarlas, con el consiguiente uso fraudulento de las mismas.

Bankinter NUNCA le solicitará que informe de sus claves o datos a través de correo electrónico o por teléfono.

8.- Compruebe su última conexión. Bankinter, a través de su transaccional le informa de la última conexión registrada con éxito en el sistema.

9.- Cuando acabe de operar utilice la función "Desconectar" (•), diseñada específicamente para informar al sistema de que su conexión ha finalizado. En caso de no utilizarla los sistemas de Bankinter están diseñados para realizar una desconexión automática, pero transcurridos 20 minutos de inactividad.

10.- Ante cualquier duda o comentario consulte con nosotros. Acceda a las páginas de seguridad y revise la totalidad de consejos y recomendaciones que allí se exponen. Si necesita más información, utilice el servicio de ebankinter responde, igualmente disponible desde nuestra web.