SEGURIDAD DE LOS SERVICIOS DE PAGO POR INTERNET

En cumplimiento de las recomendaciones emitidas por el Banco Central Europeo sobre la seguridad en los pagos efectuados por internet, El/los CLIENTE/S quedan informados de las siguientes disposiciones:

La Entidad es la responsable de implementar las medidas necesarias para mejorar la seguridad en los pagos por internet, sin embargo El/los CLIENTE/S deberán adoptar determinadas medidas que igualmente ayudarán a que las transacciones por internet sean más seguras.

Medidas a adoptar por El/los CLIENTE/S para mejorar la seguridad en los pagos por internet:

El/los CLIENTE/S deberán utilizar un equipo que disponga de antivirus y actualizarlo cuando corresponda, deberán asegurarse que se están conectando a la banca electrónica a través de una conexión segura (https y TLS), así como actualizar el navegador e instalar los parches del sistema operativo. Una vez que se finaliza la operación, deberán cerrar siempre la sesión y el navegador para finalizar correctamente las operaciones online. El modo de conexión a la banca no deberá ser a través de Wifi´s públicas o no securizadas adecuadamente.

Credenciales:

La claves de acceso a la banca electrónica deberán ser cambiadas periódicamente y siempre que se intuya que pueden ser conocidas por otras personas. No se recomienda utilizar claves repetitivas que puedan ser descubiertas fácilmente por sí mismas.

Respecto a la operativa y las medidas implementadas por la Entidad tanto en la Banca Electrónica como en las tarjetas utilizadas para efectuar pagos por Internet, El/los CLIENTE/S deberán estar informados, al menos, de los siguientes aspectos:

Para efectuar cualquier transacción por internet, El/los CLIENTE/S deberán acceder a la banca electrónica o bien a la banca telefónica a través de unas claves de acceso (usuario, NIF, contraseña). En el supuesto de la banca telefónica, se deberá indicar el Pin telefónico previamente facilitado por la Entidad.

Dichas claves de acceso serán facilitadas por la Entidad bien en la Oficina o bien serán recibidas en el domicilio indicado por El/los CLIENTE/S, debiendo cambiar la contraseña en el primer acceso que se produzca a la banca electrónica.

Determinadas operaciones que exijan un mayor nivel de seguridad, por ejemplo las transferencias, requerirán un sistema de doble autenticación.

La primera coordenada se debe introducir en la pantalla de confirmación de datos. Una vez que la banca electrónica verifique la validez de la misma, requerirá que se introduzca una segunda coordenada o una clave que le será enviada a su teléfono móvil, como segundo factor de firma de su operación en aquellas operativas que así lo exijan.

En lo que respecta a las tarjetas, estas serán remitidas al titular al domicilio proporcionado a la entidad en el momento de la contratación o en su caso a la oficina habitual del titular que se pondrá en contacto con el cliente para su recogida.

El número secreto (PIN) se remitirá por separado al domicilio del cliente o en su caso podrá entregarse en la oficina al cliente si lo solicita de forma expresa.

El número secreto (PIN) podrá ser modificado por el titular en cualquier cajero automático de la Entidad.

Respecto de las compras por Internet, La Entidad ha reforzado seguridad con el servicio de Pago Seguro por Internet.

Con este servicio, cada vez que El/los CLIENTE/S inicien una compra en un comercio seguro en Internet, identificado por los distintivos "Verified by Visa" o "Mastercard Secure Code", se recibirá en el teléfono móvil una clave numérica que deberá teclearse en la página web del comercio online para poder autenticar la compra, como segundo factor de firma de la misma.

Operativas disponibles para El/los CLIENTE/S

Se informa igualmente, que El/los CLIENTE/S tienen a su disposición determinados servicios que le permiten tener un mayor control y seguimiento de las transacciones efectuadas por internet. Uno de estos servicios es el servicio de Alertas SMS/Mail en el que se informa de cualquier movimiento que se produzca las cuentas o tarjetas de El/los CLIENTE/S, dicho servicio podría ser activado en las Oficinas de la Entidad o bien en la Banca Electrónica.

Si El/los CLIENTE/S prefieren recibir notificaciones al instante en el teléfono móvil, podrá activarse el Servicio de Avisos directamente desde la aplicación móvil de la banca electrónica.

A través de la banca electrónica, El/los CLIENTE/S podrán bloquear/ desbloquear las operaciones de transferencias a través del teléfono móvil. Con ello, se limitará el acceso a la banca electrónica sólo para modo consulta.

Para poder utilizar el servicio debe tener dado de alta un número de teléfono móvil y activar el servicio de Bloqueo Firma Operaciones por SMS en la banca electrónica. A partir de ese momento, cada vez que El/los CLIENTE/S quieran realizar una transferencia deberá desactivar el servicio, enviando un mensaje SMS o bien accediendo con su DNI-Electrónico. Este servicio podrá ser activado enviando un mensaje SMS al número 217720.

Una vez realizada la operación para bloquear el servicio inmediatamente se deberá volver a enviar un mensaje de texto.

Otra medida que existe a disposición de El/los CLIENTE/S es la opción de desactivar la modalidad de pago por internet para las tarjetas, de tal forma que esa tarjeta no sea operativa y no se pueda efectuar ninguna transacción por internet con la misma. Esta medida, podrá ser solicitada en cualquier oficina de la Entidad.

Pérdida o robo de credenciales

Si El/los CLIENTE/S desconocen o no recuerdan las claves de acceso, se deberá acudir a la oficina habitual donde se facilitarán nuevas claves
En el supuesto de que El/los CLIENTE/S hayan sufrido un robo o pérdida de las credenciales de seguridad, se deberá llamar a la mayor brevedad posible al 902 310 902.

La Entidad procederá a bloquear el usuario por motivos de seguridad, para que nadie pueda acceder con el mismo, y se volverán a emitir nuevas claves de acceso que serán remitidas por los medios habituales.

Si el El/los CLIENTE/S tienen sospechas de que han sido víctimas de un fraude en la banca electrónica o han hecho un uso indebido de sus tarjetas, además de comunicarlo a la Entidad, es conveniente que se ponga inmediatamente la denuncia correspondiente ante las autoridades competentes: Guardia Civil, Grupo de Delitos Telemáticos y Policía Nacional, Unidad de Investigación Tecnológica.

Si por el contrario es la Entidad quien detecta alguna operación sospechosa en la banca electrónica o en el uso de sus tarjetas, se disponen de herramientas de prevención contra el fraude que detectan dichas operaciones, activando un protocolo para garantizar la seguridad en el que inmediatamente se informa a El/los CLIENTE/S, pudiendo incluso llegar a bloquear temporalmente el instrumento de pago concreto en caso de no poder localizar a El/los CLIENTE/S.

Respecto a las tarjetas, El/los CLIENTE/S deberán tener presentes las siguientes recomendaciones de uso y seguridad de tarjetas: se deberá firmar la tarjeta en el reverso cuando se reciba, se deberá memorizar el nº PIN y no utilizar el mismo nº para todas las tarjetas ni revelarlo a terceros, en el caso de renovación de la tarjeta una vez recibida, se deber proceder a destruir la caducada así como comprobar periódicamente los extractos de su cuenta y guardar los recibos de compra, denunciar cualquier cargo indebido en su cuenta.
Ante cualquier robo, extravío o uso indebido de la tarjeta, así como de la tarjeta de coordenadas por terceros, El/los CLIENTE/S deberán ponerse en contacto telefónico de manera inmediata en los teléfonos 902 123 209 (si llama desde España) y (34) 91 334 67 82 (si llama desde el extranjero). Se comprobarán los datos de El/los CLIENTE/S y se bloqueará la tarjeta, indicando los pasos a seguir.

En cuanto a las **medidas de seguridad** que dispone la **banca electrónica**, El/los CLIENTE/S quedan informados de los siguientes aspectos:

La información relacionada con el acceso a la cuenta viaja de forma cifrada utilizando TLS a 256 bits. Actualmente es el sistema más potente de protección de datos de un sitio Web y está avalado por un certificado emitido por Verisign.

La banca electrónica puede estar dividida por lo menos en dos partes, la parte superior que incluye la cabecera y la parte inferior que es donde se deben introducir las claves de acceso y donde posteriormente se presenta la información ofrecida por el servicio de Banca por Internet.

La parte superior no viaja al ordenador de El/los CLIENTE/S utilizando el protocolo TLS, ya que no contiene información confidencial. La parte inferior viaja utilizando el protocolo TLS, por lo que tanto la información solicitada para la identificación, como la información relacionada con los productos financieros, viajan de forma segura.

Para que El/los CLIENTE/S puedan comprobar que la página es segura, se deberá prestar atención a que la página de dirección web sea https. Esta última "s" indica que es una página de confianza para realizar las gestiones financieras, ya que un servidor seguro comienza por https y no por http.

En las últimas versiones de los navegadores, la barra del navegador muestra el icono de un candado y la barra de direcciones está sombreada en color verde. Esto indica que la página está bloqueada frente a intentos de visualización por parte de terceros, asegurando así la privacidad de El/los CLIENTE/S.

Si la barra de direcciones aparece sombreada en rojo, se debe desconfiar de dicha página, ya que ésta podría ser fraudulenta.

Si no se utiliza la última versión disponible del navegador es posible que la barra de direcciones no aparezca sombreada.

Para comprobar los certificados de seguridad de la página hay que pulsar el icono del candado que aparece al acceder a una zona segura y verificar que la fecha de caducidad y el dominio del certificado están vigentes.

Igualmente, tienen disponible diversas páginas en las que se informan de medidas de seguridad recomendables para los clientes, como puede ser: https://www.osi.es/.

Para mayor información, puede consultar el apartado de Recomendaciones de Seguridad de en www.ruralvia.com.