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, Colonya Caixa Pollença (en adelante, la Entidad) informa a sus clientes 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 los clientes deben adoptar determinadas medidas que igualmente ayudarán a que las transacciones por internet sean más seguras.

Medidas a adoptar por los clientes para mejorar la seguridad en los pagos por internet

Los clientes deben utilizar un equipo que disponga de antivirus y actualizarlo cuando corresponda, deben asegurarse de que se están conectando a la banca electrónica a través de una conexión segura (https y TLS), así como actualizar el navegador e instalar las actualizaciones del sistema operativo. Una vez se finaliza la operación, deben cerrar siempre la sesión y el navegador para finalizar correctamente las operaciones online. La conexión al servicio de banca electrónica no debe realizarse a través de redes públicas o no securizadas adecuadamente.

Acceso a banca electrónica

La claves de acceso a la banca electrónica deben 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.

Para efectuar cualquier transacción utilizando la banca a distancia, los clientes deben acceder a la banca electrónica o bien a la banca telefónica a través de unas claves de acceso (usuario, NIF/NIE, contraseña). En el supuesto de la banca telefónica, se debe indicar el Pin telefónico previamente facilitado por la Entidad.

Dichas claves de acceso son facilitadas por la Entidad, bien en la oficina o vía SMS, 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, requieren un sistema de doble autenticación.

La primera clave que debe introducir el cliente es su clave de firma personal que el sistema le solicite. Una vez que la banca electrónica verifique la validez de la misma, requerirá que se introduzca una segunda clave que le será enviada a su teléfono móvil, como segundo factor de firma de su operación en aquellas operativas que así lo exijan.

Tarjetas de débito y de crédito

En referencia a las tarjetas, estas deben ser recogidas personalmente por los clientes en su oficina habitual.

El número secreto (PIN) se remite vía SMS desde la oficina o se puede obtener a través del servicio de duplicado de pin en la Banca Electrónica.

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

Respecto de las compras por Internet utilizando las tarjetas de Colonya, la Entidad ha reforzado seguridad con el servicio de Pago Seguro por Internet. Con este servicio, cada vez que los clientes inicien una compra en un comercio seguro en Internet, identificado por los distintivos "Verified by Visa" o "Mastercard Secure Code", según el sistema de autenticación elegido por el titular de la tarjeta, recibirá orden de autenticación biométrica a través de la aplicación de banca electrónica de la entidad, o bien un reto por SMS en el teléfono móvil para hallar la clave numérica que deberá teclearse en la página web del comercio online para poder autenticar la compra.

Operativas disponibles para los clientes

Los clientes tienen a su disposición 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 en el que se informa de cualquier movimiento que se produzca las cuentas o tarjetas de los clientes. Dicho servicio puede ser activado en las oficinas de la Entidad o bien en la Banca Electrónica.

Otra medida que existe a disposición de los clientes 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, puede ser solicitada en cualquier oficina de la Entidad y desde la propia Banca Electrónica.

Pérdida o robo de credenciales. Comunicación de fraudes.

Si los clientes desconocen o no recuerdan las claves de acceso a Banca Electrónica, se debe acudir a la oficina habitual donde se facilitarán nuevas claves, o bien, puede obtener las claves de acceso desde la pantalla de login de Banca Electrónica.

En el supuesto de que los clientes hayan sufrido un robo o pérdida de las credenciales de seguridad, se debe llamar a la mayor brevedad posible al **912 753 263**

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 los clientes 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 pongan 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 las tarjetas, a través de las herramientas de prevención contra el fraude que detectan dichas operaciones, se activa un protocolo para garantizar la seguridad en el que inmediatamente se informa a los clientes, pudiendo incluso llegar a bloquear temporalmente el instrumento de pago concreto en caso de no poder localizar a los clientes.

Recomendaciones de uso de las tarjetas

Los clientes deben tener presentes las siguientes recomendaciones de uso y seguridad de tarjetas:

- Firmar la tarjeta en el reverso cuando se reciba,
- Memorizar el PIN y no utilizar el mismo número para todas las tarjetas ni revelarlo a terceros
- En el caso de renovación de la tarjeta una vez recibida, se debe destruir la caducada
- Comprobar periódicamente los extractos de su cuenta
- Guardar los recibos de compra
- Denunciar cualquier cargo, indebido en su cuenta.

Ante cualquier robo, extravío o uso indebido de la tarjeta, los clientes deben ponerse en contacto telefónico de manera inmediata con el teléfono **913 346 782**. Se comprobarán los datos de los clientes y se bloqueará la tarjeta, indicando los pasos a seguir.

Medidas de seguridad de banca electrónica

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 está 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 los clientes 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 los clientes puedan comprobar que la página es segura, se debe 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 los clientes.

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 más información, puede consultar el apartado "Seguridad" de colonya.com