SEGURETAT DELS SERVEIS DE PAGAMENT PER INTERNET

En compliment de les recomanacions emeses pel Banc Central Europeu sobre la seguretat en els pagaments efectuats per internet, Colonya Caixa Pollença (d'ara en endavant l'Entitat) informa els seus clients de les següents disposicions.

L'Entitat és la responsable d'implementar les mesures necessàries per millorar la seguretat en els pagaments per internet, això no obstant, els clients hauran d'adoptar determinades mesures que igualment ajudaran a que les transaccions per internet siguin més segures.

Mesures a adoptar pels clients per millorar la seguretat en els pagaments per internet

Els clients han d'utilitzar un equip que disposi d'antivirus i actualitzar-lo quan correspongui, han d'assegurar-se que s'estan connectant a la banca electrònica a través d'una connexió segura (https i TLS), així com actualitzar el navegador i instal·lar les actualitzacions del sistema operatiu. Un cop es finalitzi l'operació, han de tancar sempre la sessió i el navegador per finalitzar correctament les operacions online. La connexió al servei de banca electrònica no s'ha de realitzar a través de xarxes públiques o que no siguin segures.

Accés a banca electrònica

Les claus d'accés a la banca electrònica s'han de canviar periòdicament i sempre que s'intueixi que puguin ser conegudes per altres persones. No es recomana utilitzar claus repetitives que puguin ser descobertes fàcilment per si mateixes.

Per efectuar qualsevol transacció utilitzant la banca a distància, els clients han d'accedir a la banca electrònica o bé a la banca telefònica a través d'unes claus d'accés (usuari, NIF/NIE, contrasenya). En el supòsit de la banca telefònica, s'ha d'indicar el Pin telefònic prèviament facilitat per l'Entitat.

Les esmentades claus d'accés són facilitades per l'Entitat, bé a l'oficina o via SMS, havent de canviar la contrasenya en el primer accés que es produeixi a la banca electrònica.

Determinades operacions que exigeixin un major nivell de seguretat, per exemple, les transferències, requeriran un sistema de doble autenticació.

La primera clau que ha d'introduir el client és la seva clau de signatura personal que el sistema li sol·liciti. Un cop que la banca electrònica verifiqui la validesa d'aquesta, requereix que s'introdueixi una segona clau que li serà enviada al seu telèfon mòbil, com a segon factor de signatura de la seva operació en aquelles operatives que així ho exigeixin.

Targetes de dèbit i de crèdit

En referència a les targetes, aquestes han de ser recollides personalment pels clients a la seva oficina habitual.

El número secret (PIN) es remet via SMS des de l'oficina o es pot obtenir a través del servei de duplicat de pin a la Banca Electrònica.

El número secret (PIN) pot ser modificat pel titular en qualsevol caixer automàtic de l'Entitat.

Respecte de les compres per Internet utilitzant les targetes de Colonya, l'Entitat ha reforçat seguretat amb el servei de Pagament Segur per Internet. Amb aquest servei, cada vegada que els clients inicïin una compra en un comerç segur en Internet, identificat pel distintiu "Verified by Visa" o "Mastercard Secure Code", segons el sistema d'autenticació triat pel titular de la targeta, rebrà ordre d'autenticació biomètrica a través de l'aplicació de banca electrònica de l'Entitat, o bé un repte per SMS en el telèfon mòbil per trobar la clau numèrica que s'haurà de teclejar a la pàgina web del comerç online per poder autenticar la compra.

Operatives disponibles per als clients

Els clients tenen a la seva disposició serveis que permeten tenir un major control i seguiment de les transaccions efectuades per Internet.

Un d'aquests serveis és el d'Alertes en el qual s'informa de qualsevol moviment que es produeixi als comptes o targetes dels clients. L'esmentat servei pot ser activat a les oficines de l'Entitat o bé a la Banca Electrònica.

Una altra mesura que existeix a disposició dels clients és l'opció de desactivar la modalitat de pagament per internet per a les targetes, de tal forma que aquesta targeta no sigui operativa i no es pugui efectuar cap transacció per internet amb ella. Aquesta mesura pot ser sol·licitada a qualsevol oficina de l'Entitat i des de la pròpia banca electrònica.

Pèrdua o robatori de credencials. Comunicació de fraus

Si els clients desconeixen o no recorden les claus d'accés a Banca Electrònica, s'ha d'acudir a l'oficina habitual on es facilitaran noves claus o bé podrà obtenir les claus d'accés des de la pantalla de login de Banca Electrònica.

En el supòsit que els clients hagin sofert un robatori o pèrdua de les credencials de seguretat, han de cridar a la major brevetat possible al **912 753 263**.

L'Entitat pot bloquejar l'usuari per motius de seguretat, perquè ningú no pugui accedir-hi amb aquest i es tornaran a emetre noves claus d'accés que seran remeses pels mitjans habituals.

Si els clients sospiten que han estat víctimes d'un frau en la banca electrònica o s'ha fet un ús indegut de les seves targetes, a més de comunicar-ho a l'Entitat, és convenient que posin immediatament la denúncia corresponent davant les autoritats competents: Guàrdia Civil, Grup de Delictes Telemàtics, i Policia Nacional, Unitat d'Investigació Tecnològica.

Si, contràriament, és l'Entitat que detecta alguna operació sospitosa en la banca electrònica o en l'ús de les targetes a través de les eines de prevenció contra el frau que detecten les dites operacions, s'activa un protocol per garantir la seguretat en el qual immediatament s'informa als clients, podent inclús arribar a bloquejar temporalment l'instrument de pagament concret en cas de no poder localitzar els clients.

Recomanacions d'us de les targetes

Els clients han de tenir presents les següents recomanacions d'ús i seguretat de targetes:

- Signar la targeta en el revers quan es rebi.
- Memoritzar el PIN i no utilitzar el mateix número per a totes les targetes ni revelar-lo a tercers.
- En el cas de renovació de la targeta, un cop rebuda la nova, s'ha de destruir la caducada.
- Comprovar periòdicament els extractes del seu compte.
- Guardar els rebuts de compra
- Denunciar qualsevol càrrec indegut en el seu compte.

Cas de qualsevol robatori, pèrdua o ús indegut de la targeta, els clients han de posar-se en contacte telefònic de manera immediata amb el telèfon **913 346 782**. Es comprovaran les dades dels clients i es bloquejarà la targeta, indicant les passes a seguir.

Mesures de seguretat de banca electrònica

La informació relacionada amb l'accés al compte viatja de forma xifrada utilitzant TLS a 256 bits. Actualment, és el sistema més potent de protecció de dades d'un lloc web i està avalat per un certificat emès per Verisign.

La banca electrònica està dividida almenys en dues parts. La part superior que inclou la capçalera i la part inferior que és on s'han d'introduir les claus d'accés i on posteriorment es presenta la informació oferta pel servei de Banca per Internet.

La part superior no viatja a l'ordinador dels clients utilitzant el protocol TLS, ja que no conté informació confidencial. La part inferior viatja utilitzant el protocol TLS, pel que tant la informació sol·licitada per a la identificació, com la informació relacionada amb els productes financers, viatgen de forma segura.

Per tal que els clients puguin comprovar que la pàgina és segura, s'ha de prestar atenció a que la pàgina de direcció web sigui https. Aquesta darrera "s" indica que és una pàgina de confiança per realitzar les gestions financeres, ja que un servidor segur comença per https i no per http.

En les darreres versions dels navegadors, la barra del navegador mostra la icona d'un pany i la barra d'adreces està ombrejada en color verd. Això indica que la pàgina està bloquejada front a intents de visualització per part de tercers, assegurant així la privacitat dels clients.

Si la barra d'adreces apareix ombrejada en vermell, s'ha de desconfiar d'aquesta pàgina, ja que podria ser fraudulenta. Si no s'utilitza la darrera versió disponible del navegador, és possible que la barra d'adreces no aparegui ombrejada.

Per comprovar els certificats de seguretat de la pàgina s'ha de pitjar sobre la icona del pany que apareix a l'accedir a una zona segura i verificar que la data de caducitat i el domini del certificat són vigents.

Igualment, tenen disponibles diverses pàgines en les quals s'informa de mesures de seguretat recomanables per als clients, com poden ser: https://www.osi.es/.

Per a més informació, pot consultar l'apartat "Seguretat" de la web de l'Entitat: colonya.com