Recomendaciones para el uso seguro del servicio de Pagos por Internet

cajalmendralejo

 Noviembre 2015

El uso de Internet para nuestras acciones cotidianas es hoy día una realidad. A través de una "simple“ navegación, accedemos a nuestro portal de Banca Electrónica, consultamos nuestras últimas operaciones y saldo, modificamos datos, contratamos nuevos servicios,… Además de las acciones que realizamos a través de la plataforma de nuestra Entidad bancaria, realizamos nuestras compras de ropa, ocio, comida,… a través de Internet. A modo de resumen, se puede decir que el equipo del que hacemos uso para conectarnos a Internet se puede considerar nuestra extensión “cibernética”, por lo que su correcto funcionamiento, configuración y seguridad incidirá directamente en nuestra persona.

El uso de Internet, fundamentalmente, se basa en la confianza establecida entre nosotros como usuarios y nuestros prestadores de servicios. El gran problema que se presenta es la existencia de ciberdelincuentes que tratan de aprovecharse de esta relación de confianza con unos intereses ilícitos, los llamados “cibercriminales”.

Dentro del “mundo” cibernético no existe más riesgo que en el mundo “real” en el que nos movemos día a día. El problema proviene del desconocimiento, por parte de los usuarios, del riesgo que se genera por nuestros malos hábitos y un mal uso del servicio.

A continuación se van a detallar una serie de buenas prácticas y recomendaciones para un uso seguro de los servicios de pago por Internet por parte de nuestros clientes. Estas recomendaciones estarán agrupadas en los apartados:

Seguridad en Cajalnet.es

Acceso Seguro

A continuación se detallan una serie de medidas de seguridad que estamos aplicando en nuestro portal de cliente, para que el uso del mismo resulte lo más seguro posible:

1. Acceso al portal mediante usuario y contraseña. Recuerde proteger las claves de acceso, ya que son utilizadas para identificarse y autenticarse frente a los sistemas de **Cajalmendralejo,** por lo que es necesario que sean personales e intrasferibles. Se recomienda:
    - No utilizar claves fácilmente deducibles (cumpleaños, aniversarios, DNI,…).
    - Es recomendable cambiarlas periódicamente.

    Recuerde que **Cajalmendralejo** NUNCA solicitará sus claves o datos a través de correo electrónico o por teléfono.

2. Validación de las operaciones realizadas mediante el uso de tarjeta de coordenadas (que nunca se utilizará para el acceso al servicio) y códigos temporales (OTP) enviados a su teléfono movil mediante SMS gratuito. Estas claves enviadas mediante SMS tendrán una validez de 2 minutos, transcurridos los cuales será necesario realizar de nuevo la operación. Recuerde que desde **Cajalmendralejo** nunca se le solicitará más de una posición de la tarjeta de coordenadas para validar una operación.

Garantía de Seguridad

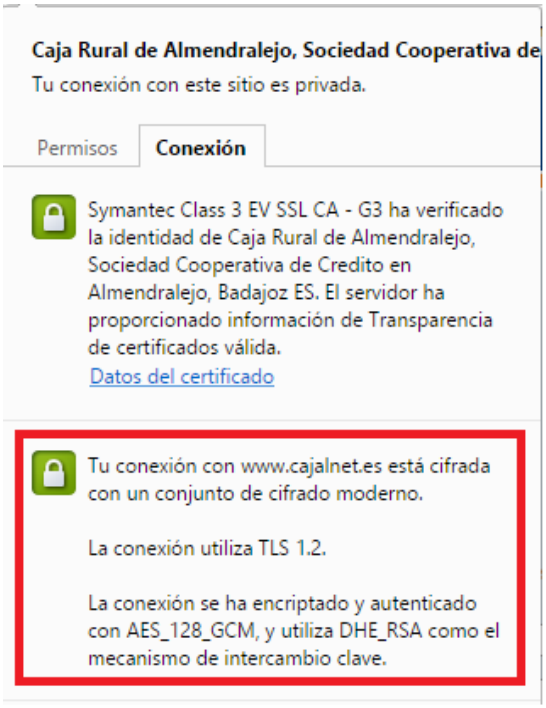
3. Para asegurarse de la autenticidad de la web de Cajalnet a la que está intentando acceder, es recomendable que periódicamente compruebe que tanto las comunicaciones son seguras como que existe un certificado digital emitido por una empresa independiente de reconocido prestigio en materia de seguridad informática y que está vigente.

    Para ello debe pulsar el icono del candado que aparece en la barra de navegación de una zona segura (http**s** y sombreado en verde) o

bien el sello emitido por la empresa de certificación de seguridad (en nuestro caso el sello de “Norton Secured”):

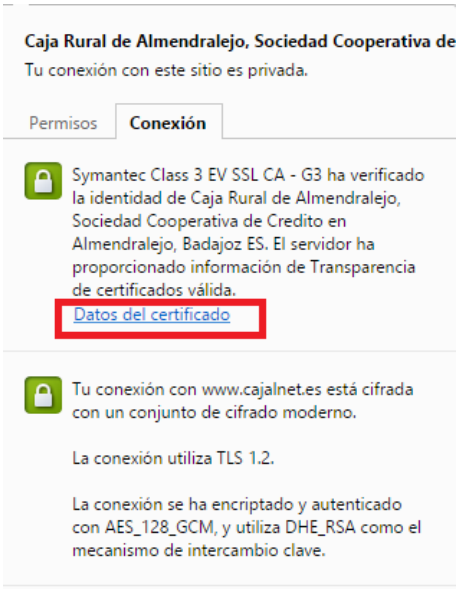
De esta forma podra verificar que empleamos:

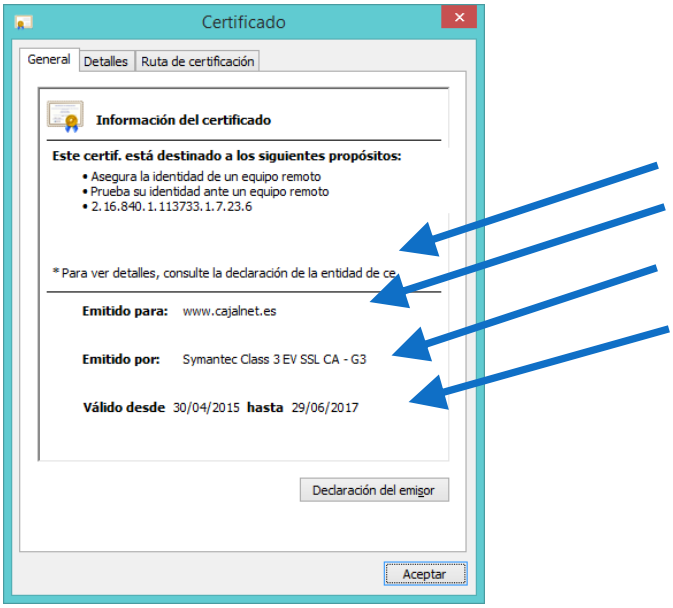
4. Cifrado de las comunicaciones utilizando **TLS 1.2,** encriptación y autenticado con **AES_128_GCM** y utiliza **DHE_RSA** como mecanismo de intercambio de claves.



5. Uso de certificados digitales que verifican la identidad de **Cajalmendralejo**. Es recomendable revisar de forma periódica el certificado con el que se firma la web, para evitar ser estafados por páginas diseñadas para el robo de datos.

A continuación, se detallan los pasos a seguir para la realización de esta acción:





- Finalidad.
- Dirección para emisión.
- Entidad certificadora.
- Validez del certificado.

6. Usar la opción de desconexión a la hora de salir de la plataforma de Banca Electrónica.

7. **Ante cualquier duda o comentario consulte con nosotros.**

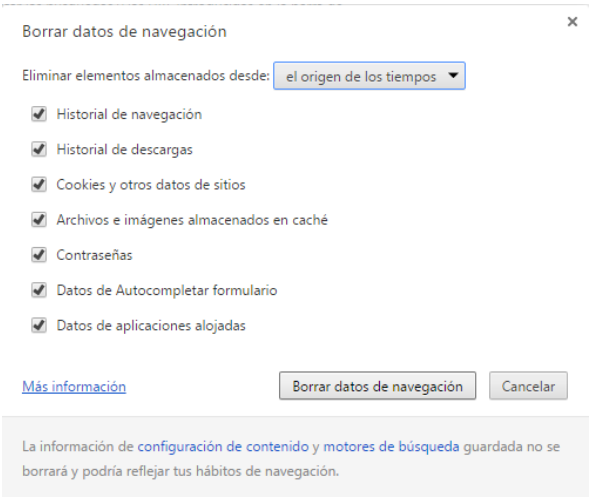
Seguridad en Tarjetas

Recomendaciones de uso

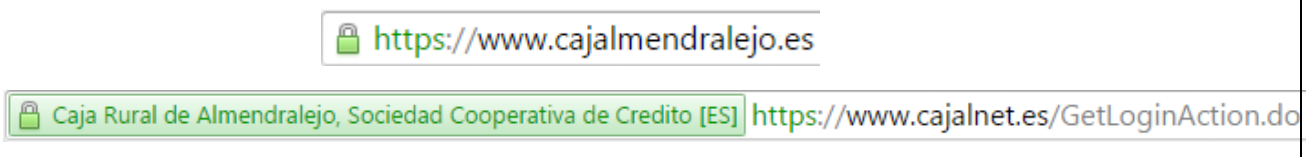
1. Firme su tarjeta en el reverso cuando la reciba.
2. Memorice su número PIN y no utilice el mismo para todas sus tarjetas.
3. Destruir siempre las tarjetas caducadas.
4. Si usted no realiza compras en Internet, deshabilite la opción de compras onlines de su tarjeta.
5. Denuncie cualquier cargo indebido en su cuenta.
6. En caso de robo o pérdida de su tarjeta, póngase en contacto inmediantemente con nosotros en el teléfono **902 300 148.**
7. Para operaciones con tarjeta de débito o crédito la clave OTP sustituirá al código PIN cuando las compras se realicen en comercios electrónicos seguros, identificados por:
    - En el navegador aparece una llave o candado en color verde.
    - El nombre de la página comienza por https.
    - Aparece, al menos, uno de los siguientes símbolos:

Seguridad en la Navegación

En este apartado se van a establecer una serie de buenas prácticas y recomendaciones para que la navegación a través de Internet resulte lo más segura posible, y tratar así de mitigar o prevenir los riesgos que se puedan producir.



1. Eliminar los ficheros temporales para evitar que las páginas por las que se navega queden almacenadas en la memoria del navegador.
2. Desactivar la opción de guardar o autocompletar la contraseña en el navegador.
3. Actualizar periódicamente el navegador que utilizamos para conectarnos a Internet.
4. Evitar, en la medida de lo posible, acceder a los servicios de Banca Electrónica (y otros que requieran usuario y contraseña) desde equipos o conexiones públicas, donde el acceso y la conexión a Internet están disponibles para varias personas.
5. Cuando se realiza una conexión sobre el servicio de Banca Electrónica, comprobar que en el navegador la URL empieza por **https://** y no por **http://.** Mediante el uso de conexiones seguras, se garantiza que todo el tráfico que se genera viaja cifrado.



6. INTECO (Instituto Nacional de Tecnologías de la Información) ofrece un listado de herramientas gratuitas que ayudarán a proteger nuestro equipo. Este listado se presenta a través de la web de OSI en la siguiente URL: http://www.osi.es/es/herramientas-gratuitas.

Ataques más frecuentes

Phishing

El **phishing** es un tipo de ataque, mediante el cual los ciberdelincuentes se hacen pasar por otra persona u organización (ingeniería social) para tratar de engañar a sus víctimas y así obtener cierta información de ellas. Algunas recomendaciones para no ser víctima de este tipo de ataques:

1. Revisar la dirección desde la que se reciben los correos electrónicos, para comprobar si realmente se trata de **Cajalmendralejo**.
2. No abrir ningún correo ni archivos adjuntos si duda de la procedencia de los mismos.
3. No acceder a ninguno de los enlaces que aparezcan en estos correos. A través de los mismos se puede instalar malware en sus dispositivos para acceder a su información personal. Siempre que vaya hacer uso de la plataforma de Banca Electrónica, introduzca manualmente la URL o a través de la funcionalidad de favoritos del navegador.
4. **RECUERDE!!!** Desde **Cajalmendralejo** **NUNCA** solicitaremos sus datos de acceso a la web, tarjeta de coordenadas o códigos OTP mediante mail o de forma telefónica. Estos datos sólo serán solicitados a través de nuestra plataforma de Banca Electrónica y sólo uno por operación.

5. En resumen, las preguntas que debe hacerse para detectar un correo malintencionado:
    - **¿El contenido es sospechoso?** Sea precavido ante correos que indican que la cuenta ha sido bloqueada o cancelada, que anulen una transferencia que usted no ha realizado, …
    - **¿La escritura es correcta?** Si hay errores en el texto, como fallos semánticos, palabras con símbolos extraños, frases mal redactadas,…sospeche de la fiabilidad del correo.

- **¿El correo va personalizado?** Su Entidad conoce su nombre. Si recibe comunicaciones anónimas dirigidas a “Notificación a usuario” o “Querido amigo”, es un indicio que le debe poner en alerta.
- **¿Es necesario hacer algo urgente?** Si nos obliga a tomar una decisión en poco tiempo, no es buena señal. Póngase en contacto con nosotros para validar la urgencia y veracidad.
- **¿El enlace es real?** Observe si el texto del enlace coincide con la dirección a la que apunta.
- **¿Quién envía el correo?** Si recibe la comunicación de un buzón de correo tipo @gmail.com o @hotmail.com, ¡sospeche!
- **¿Qué tipo de información le piden?** Se le solicitan datos de sus productos bancarios y datos personales, como su móvil, DNI, … podría ser un correo fraudulento.

Smishing

El Smishing es una variante del phishing tradicional, que en lugar de hacer uso del envío de correos electrónicos utiliza los mensajes SMS. Mediante el envío de un SMS al móvil, se intenta convencer al usuario para que visite una página fraudulenta o llame a algún número de teléfono, con el objetivo de obtener sus claves de banca electrónica, datos financieros,…

A continuación, le indicamos una serie de consejos básicos para evitar ser víctima de un Smishing:

- No acceda a ningún enlace que llegue a través de SMS.
- No proporcione usuarios, claves, datos bancarios o personales a través de SMS.
- No almacene información personal o bancaria en su móvil.

Virus Informáticos

Los virus informáticos son programas que se instalan en el PC, Tablet o Smartphone sin el permiso o conocimiento del propietario con fines maliciosos, como robar o destruir información.

Las consecuencias más importante si es atacado por un virus informático son:

- Borrado de información.
- Robo de información.
- Suplantación de identidad.
- Pérdidas económicas.

Los síntomas en los dispositivos infectados son:

- Realización de operaciones de forma más lenta.
- Mayor tiempo a la hora de ejecutar y cargas programas.
- Disminución del espacio libre en del disco duro y de la memoria RAM disponible
- Aparición de programas desconocidos en la memoria.

Las principales vías de entrada de estos software maliciosos son:

- Correo electrónico.
- SMS.
- Dispositivos de almacenamiento externos (memorias USB, dicos duros, tarjetas de memoria,...)
- Descarga de ficheros.
- Páginas web maliciosas.
- Redes Sociales.

Medidas de protección:

- Sea prudente al visitar sitios webs desconocidos y vigile la descarga de ficheros o programas.
- No almacene ni ejecute en su dispositivo programas de los que no conozca su origen.
- Mantenga actualizado su sistema operativo.
- Utilice sistemas antivirus.
- Verifique los documentos que haya podido recibir del exterior.
- Haga copias de seguridad con cierta frecuencia, para evitar la pérdida de datos importantes.
- Utilice herramientas de seguridad como:
    - **Programas de bloqueo de ventanas emergentes.**
    - **Programas de bloqueo de banners.**
    - **Programas anti-spam.**
    - **Programas anti-fraude.**

Seguridad en tu equipo

Otro punto importante a destacar dentro de la seguridad es nuestro propio equipo, que va desde el sistema operativo en el que está basado hasta el sofware que tenemos instalado en el mismo. Para tener un mínimo de seguridad en nuestros equipos, es recomendable realizar las siguientes tareas:

1. Actualizar periódicamente el sistema operativo del equipo debe convertirse en una tarea asídua por parte del usuario. Disponer de un sistema operativo no obsoleto es un requerimiento necesario para evitar ser víctima de las nuevas vulnerabilidades que van apareciendo cada día en los mismos y que son explotadas con fines delictivos.
2. Al igual que es recomendable actualizar el sistema operativo del equipo, tambiés es muy importante actualizar el software instalado en el mismo. Concretamente, para lo que nos atañe en nuestro caso, el software que utilizamos para conectarnos a los servicios bancarios es el navegador, por lo que es **importantísimo** tener siempre la última versión del mismo. Esta tarea es muy secilla de realizar y sólo llevará unos minutos, consiguiendo evitar ataques que hacen uso de versiones de software con vulnerabilidades conocidas.
3. Si no lo usas, elimínalo. Si es importante mantener actualizado el software que utilizamos en nuestro sistema, igual de importante es eliminar aquellas aplicaciones de las que no hacemos uso y que se pueden convertir en una puerta de entrada de un atacante.
4. El uso de un antivirus es esencial y éste debe ser actualizado periódicamente para que, así, resulte eficaz en la defensa del equipo. Disponer de un software antivirus nos puede ayudar frente a ataques y software malicioso.
5. Hacer uso de Firewall. Estos sistemas bloquean el tráfico haciendo uso de unas reglas previamente definidas. Por defecto, en los sistemas Windows este sistema de seguridad viene activado y con unas reglas básicas precargadas. Es posible que en algunos casos, el Firewall sea gestionado por el antivirus que usemos.
6. Hacer uso de contraseñas para desbloquear el equipo, de esa forma evitaremos accesos no autorizados al mismo.

Recomendaciones Básicas

Le resumimos las recomendaciones más importantes que debe observar para operar con seguridad en Internet:

- **El usuario y la contraseña son claves personales e intransferibles.** Para poder garantizar la seguridad es preciso mantener la confidencialidad de estos datos. Le recomendamos no utilizar contraseñas triviales o de fácil deducción, ni cederlas a terceros, así como su modificación periódica.
- **No facilite datos personales o financieros.** No es recomendable que se faciliten datos personales o financieros si no está en un entorno seguro y con proveedores de confianza.
- **No facilite sus claves ni números secretos.** El usuario será responsable de todas las acciones que realice con sus claves de acceso. Por ello no debe facilitar sus códigos en entornos que no sean de Cajalmendralejo, ni aun cuando utilizando canales alternativos (correo electrónico, teléfono, etc.) se identifiquen como Cajalmendralejo o Caja Rural de Almendralejo con propuestas engañosas, promociones o regalos, y errores técnicos que obliguen a modificar esas claves bajo petición de las actuales ya que Cajalmendralejo **NUNCA** solicitará ningún dato personal a través de correo.
- **No debe aceptar documentos ni archivos provenientes de desconocidos.** Pueden ser una vía de acceso a peligrosos VIRUS muy perjudiciales para su sistema operativo. Por ello, si el emisor es alguien poco fiable o de dudosa credibilidad no debe acceder a documentos adjuntos ni pinchar sobre ningún enlace que pueda contener el correo. Además, es importante instalar un sistema antivirus, utilizarlo y actualizarlo periódicamente.
- **Recuerde que NUNCA le solicitaremos sus datos.** Por su seguridad **NUNCA** le solicitaremos sus datos personales, financieros y/o claves personalmente, por medio de correos o vía telefónica. En el caso de

que se les solicitara los datos por alguno de estos medios póngase inmediatamente en contacto con su Entidad.

- **Recuerde que <u>NUNCA</u> le solicitaremos sus coordenadas si no es para firmar una operación que haya realizado dentro de Cajalnet.** Tenga en cuenta que determinadas operaciones que exijan un mayor nivel de seguridad requerirán un sistema de doble autenticación, pudiendo solicitarle una clave enviada a su teléfono móvil mediante SMS (OTP). Si se le requiere algo diferente en algún momento, desconfíe y póngase en contacto con su oficina habitual a través del teléfono 902 300 148, ya que puede tratarse de un intento de fraude.
- **Evite usar equipos públicos o compartidos,** así como lugares donde pueda ser observado.
- **Redes sociales. No exponga sus datos publicados en su perfil a terceras personas** y/o desconocidos.
- **Utilice el botón de desconexión.** Siempre que desee abandonar Cajalnet, es recomendable utilizar el botón “Salir de la Banca”, situado en la esquina superior derecha de la pantalla, para salir del sistema con el menor riesgo.
- **Hágase con software actualizado.** Utilice software anti-virus y toda clase de programas de protección actuales para su ordenador teniendo precaución de que no queden desfasados.

Glosario

- **Certificado electrónico o digital:** Documento digital emitido por una entidad independiente que garantiza la identidad de los sistemas y de las personas en internet. Un certificado electrónico sirve para autenticar la identidad de un usuario, firmar electrónicamente para garantizar la integridad de los datos y cifrar los datos.
- **Cifrado:** El cifrado es un método que permite aumentar la seguridad de un mensaje o de archivo mediante la codificación del contenido para que sólo sea leído por la persona que disponga de la clave de cifrado adecuada para decodificarla.
- **Código malicioso:** El malware es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. Existen distintas familias de malware, como son: virus, gusanos, troyanos, backdoor, ransomware,..
- **Cookie:** Información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.
- **Cortafuego o firewall:** Herramienta informática diseñada para bloquear el acceso no autorizado dentro de un red.
- **Criptografía:** Algoritmos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidad que se comunican.
- **Firma electrónica:** Información digital asociada a una operación en particular realizada en internet que, junto con los certificados, permite garantizar la identidad de los participantes en una transacción.
- **Ingeniería social:** Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal.
- **Intrusión:** Ataque informático en el que el atacante consigue obtener un control completo sobre la máquina. El atacante puede obtener y alterar todos los datos de la máquina, modificar su funcionamiento e incluso atacar nuevas máquinas.
- **Spyware:** Aplicación maliciosa o engañosa que se instalan de forma oculta junto con otros programas que se descarga el usuario.