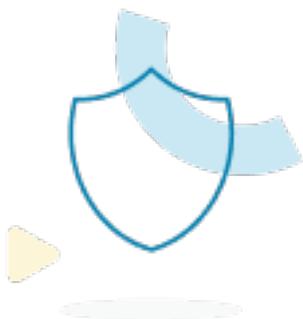


Caixabank

Gestiona cómodamente tus solicitudes de pago de recibos devueltos

Accede a CaixaBankNow, tu banca digital y acepta o rechaza las solicitudes de pago enviadas por las entidades. Puedes elegir la cuenta con la que prefieres pagar o el motivo de rechazo en caso de que no aceptes la solicitud.

Con Solicitud de Pago todo son ventajas



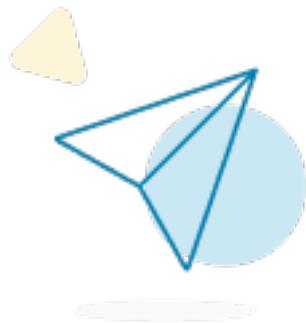
Entorno de pago seguro y transparente.



Recibe solicitudes de pago personalizadas y contextualizadas.



Realiza pagos cualquier día, a cualquier hora y mediante transferencia inmediata¹ gratuita.



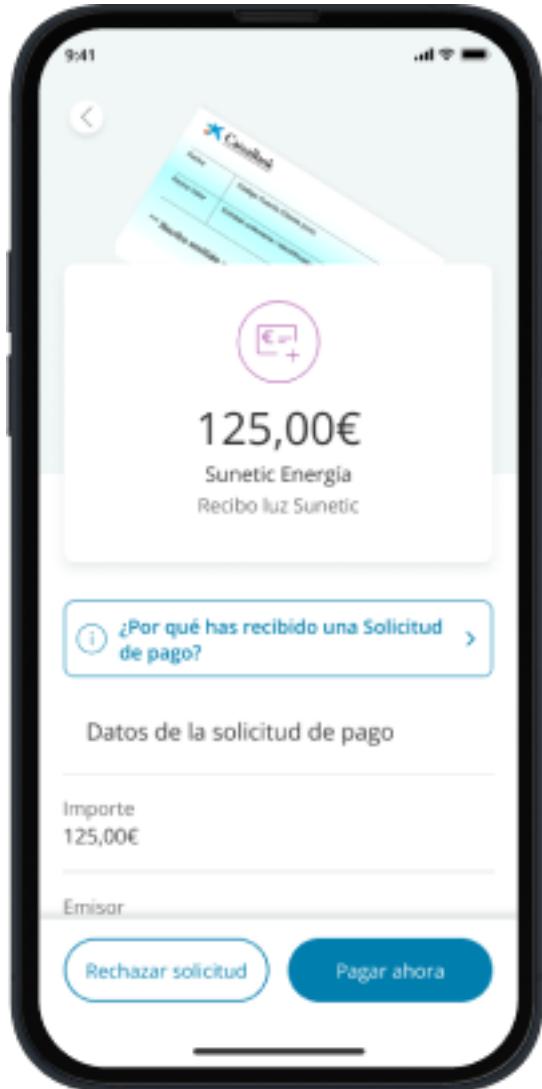
Comunicación rápida, online y directa entre el beneficiario y el destinatario.

¿Cómo funciona el servicio de Solicitud de Pago?



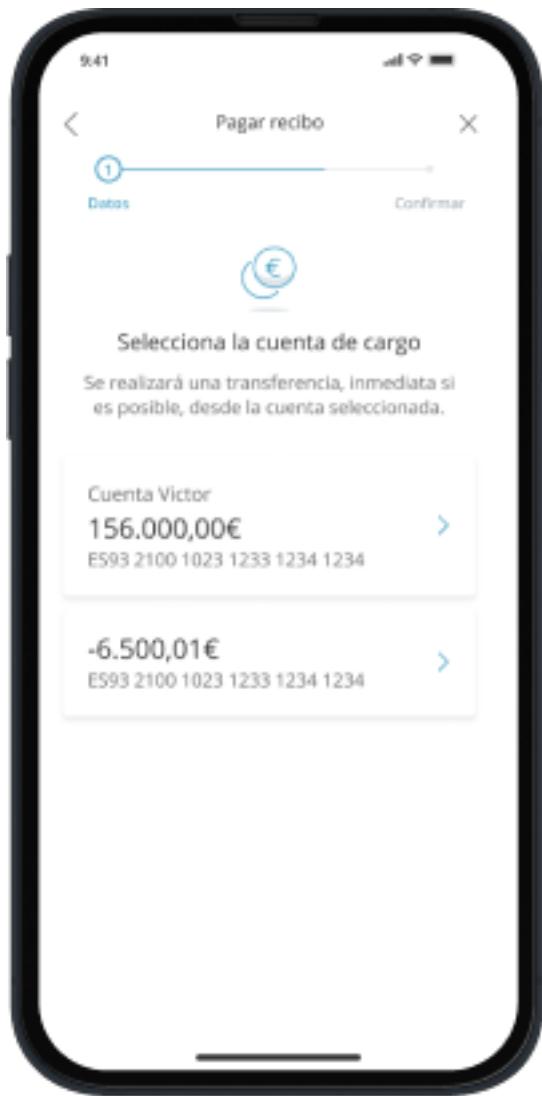
Recibe un aviso

Mediante **notificación móvil** te avisaremos que tienes una solicitud de pago pendiente que debes gestionar.



Entra en CaixaBankNow, tu banca digital

Revisa los datos de la solicitud de pago y **acepta o rechaza²** el pago.



Selecciona la cuenta

Tras aceptar el pago, selecciona la cuenta de cargo. Se realizará una **transferencia inmediata¹ gratuita** con el importe del recibo.



Firma la operación

Comprueba que los datos sean correctos y **confirma la operación**.

Preguntas frecuentes sobre la solicitud de pagos

¿Qué es una solicitud de pago?

Es una notificación por la que un emisor solicita un pago a un cliente.

¿Por qué has recibido una solicitud de pago?

La entidad emisora te envió un recibo previamente, el cual fue devuelto por alguna razón. Ahora, solicita que realices el pago del recibo antes de una fecha concreta.

¿Es seguro?

Sí, accede a CaixaBankNow para realizar la operación con total seguridad.

¿Tiene algún coste?

No, el servicio es gratuito, tanto si aceptas, rechazas o caduca la solicitud de pago.

¿Tienes que darte de alta?

No. Si un emisor te envía una solicitud de pago simplemente recibirás la notificación.

¿Cómo se gestiona una solicitud de pago?

Si estás de acuerdo, puedes pagar dentro de la fecha límite. Solo tienes que pulsar en el botón Pagar ahora , seguir los pasos y el pago se realizará.

Si no estás de acuerdo, puedes rechazar la solicitud de pago. Pulsa el botón Rechazar solicitud o simplemente deja que pase la fecha límite. Podrás indicar un motivo de rechazo, solo lo comunicaremos a la entidad si nos autorizas.

¿Qué pasa si rechazas la solicitud de pago?

No se emitirá el pago y se le informará al emisor que su solicitud ha sido rechazada. Podrás elegir entre los motivos de rechazo disponibles.

¿Qué pasa si caduca la solicitud de pago?

No se emitirá el pago y se le informará al emisor que su solicitud ha caducado.

¿Cuánto tiempo hay para gestionar una solicitud de pago?

El plazo de caducidad estará especificado en la solicitud de pago.

¿Qué ocurre si aceptas la solicitud de pago?

Si aceptas, se realizará el pago por medio de una transferencia inmediata, siempre que sea posible.

¿Se puede solicitar una devolución?

No. Una vez aceptada la solicitud, no se podrá realizar una devolución.

¿Podré volver a recibir una solicitud de pago ya gestionada?

No, una vez se haya gestionado no volverás a recibir una solicitud por el mismo concepto. Si necesitas más información, contacta con el emisor.

Preguntas frecuentes sobre el nuevo Mis Tarjetas

¿Dónde puedo visualizar el detalle de los últimos movimientos de Mis Tarjetas?

Para visualizar los últimos movimientos que se hayan producido en tus tarjetas accede a "Mis Tarjetas" de tu banca digital CaixaBankNow. Al clicar sobre el movimiento podrás consultar el detalle. Para cada movimiento se detallan datos tales como: movimiento, fecha, importe, saldo...

¿Cómo consultar mis medios de pago?

Para consultar todos tus medios de pago asociados a cada uno de tus contratos, tales como tarjetas físicas o virtuales, accede a "Mis Tarjetas" en tu banca digital CaixaBankNow.

¿Cómo bloquear y desbloquear Mis Tarjetas?

Para bloquear tu tarjeta en tu banca digital CaixaBankNow accede a "Mis Tarjetas" y desde la pestaña de opciones, haz clic en "Bloquear tarjeta".

Para desbloquear tu tarjeta en tu banca digital CaixaBankNow accede a "Mis tarjetas" y haz clic en "Desbloquear".

¿Cómo puedo reclamar una operación?

Para reclamar una operación accede a tu banca digital CaixaBankNow y en el detalle del movimiento, haz clic en "Reclamar compra" o "Reclamar movimiento". Podrás reclamar operaciones duplicadas, operaciones que se hayan hecho con tu tarjeta perdida o robada, operaciones que hayas hecho con tu tarjeta y cuya mercancía o servicio que no hayas recibido, etc.

¿Cómo pagar a plazos una operación?

Para pagar a plazos una operación accede a tu banca digital CaixaBankNow y desde "Mis Tarjetas" haz clic en "Pagar a plazos". Con esta opción podrás gestionar tu dinero disponible eligiendo antes del día que movimientos de más de 40€ y de un importe inferior al disponible de tu crédito quieras pagar cómodamente en 3, 6 o 12 plazos.

¿Cómo pasar dinero de Mis Tarjetas a cuenta? (servicash)

Para pasar dinero de tu tarjeta a cuenta accede a tu banca digital CaixaBankNow y desde "Mis Tarjetas" haz clic en "Pasar a cuenta" y selecciona de qué tarjeta quieras pasar el dinero, cuánto dinero necesitas y en qué cuenta quieres que lo ingresemos.

¿Cómo puedo ver el límite que tengo en Mis Tarjetas?

Para consultar el límite de crédito de tu tarjeta asociada a un contrato accede a tu banca digital CaixaBankNow, y desde "Mis Tarjetas" haz clic en "Límite de crédito". En caso de poder modificarlo, podrás además ver el nuevo saldo disponible y el consumido.

¿Cuándo será la fecha de mi próxima liquidación?

Para consultar la fecha de tu próxima liquidación de un contrato accede a tu banca digital CaixaBankNow, y desde "Mis Tarjetas" haz clic en "Próximo pago". Podrás consultar la lista de liquidaciones, ver el detalle y reclamar las operaciones.

¿Cómo puedo cambiar mi forma de pago?

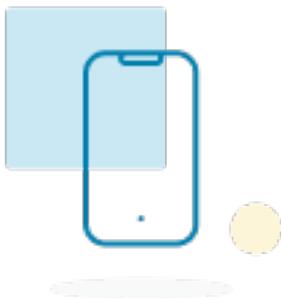
Para cambiar la forma de pago de un contrato accede a tu banca digital CaixaBankNow, y desde "Mis Tarjetas" haz clic en "Cómo pagarla" y personaliza la forma de pago. Podrás escoger lo que vayas gastando con tu tarjeta y con qué frecuencia quieras liquidar la deuda.

¿Cómo puedo avanzar el pago de la deuda pendiente?

Para avanzar el pago de la deuda pendiente en tu banca digital CaixaBankNow, y desde "Mis Tarjetas" haz clic en "Avanzar pago" desde la pestaña "Opciones". Esto te va a permitir aumentar el disponible actual, seleccionando la tarjeta a la que le quieras restaurar el límite de crédito introduciendo el importe que deseas avanzar, y seleccionando la cuenta de cargo.

Paga, envía y recibe dinero fácilmente con tu móvil con Bizum

Bizum es un servicio gratuito de pagos que puedes usar a través de la app de CaixaBankNow que permite enviar y recibir dinero entre particulares, pagar online desde la web de un comercio o realizar donaciones a ONG.



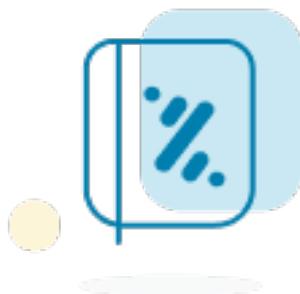
Fácil

Solo necesitas el número de teléfono.



Rápido

Realiza pagos y recibe dinero al momento.



Seguro

Utiliza Bizum desde tu aplicación CaixaBankNow con la máxima seguridad.

Anterior diapositiva

6.

Confirma la operación

Revisa los datos y pulsa “Confirmar” para enviar el dinero.

1.

Envía dinero

Es fácil e inmediato desde CaixaBankNow, tu banca digital.

2.

Entra en Bizum

En CaixaBankNow, desde la pantalla principal pulsa “Bizum”. Después, selecciona la opción “Enviar dinero”.

3.

Escoge a quién enviarlo

Puedes seleccionar un contacto de tu agenda o introducir un número de teléfono.

4.

Introduce el importe

Deberás indicar un importe de entre 0,50€ y un máximo de 500 €.

5.

Añade información para el destinatario

Obligatoriamente, deberás escribir un concepto para el envío y, adicionalmente, podrás escribir un mensaje y añadir una fotografía.

6.

Confirma la operación

Revisa los datos y pulsa “Confirmar” para enviar el dinero.

1.

Envía dinero

Es fácil e inmediato desde CaixaBankNow, tu banca digital.

Siguiente diapositiva

- 1
- 2
- 3
- 4
- 5
- 6

Anterior diapositiva

7.

Confirma la operación

Revisa los datos y pulsa “Confirmar” para solicitar el dinero.

1.

Solicita dinero

Hazlo cómodamente desde CaixaBankNow, tu banca digital.

2.

Entra en Bizum

En CaixaBankNow, desde la pantalla principal pulsa “Bizum”. Después, selecciona la opción “Solicitar dinero”.

3.

Escoge a quién solicitarlo

Puedes seleccionar varios contactos de tu agenda o introducir números de teléfono.

4.

Introduce el importe

Deberás indicar un importe a partir de 0,50€.

5.

Divide el importe

Si vas a solicitar el dinero a varias personas, selecciona cómo hacer la división.

6.

Añade información para el destinatario

Deberás escribir un concepto para el envío.

7.

Confirma la operación

Revisa los datos y pulsa “Confirmar” para solicitar el dinero.

1.

Solicita dinero

Hazlo cómodamente desde CaixaBankNow, tu banca digital.

Siguiente diapositiva

- 1
- 2
- 3
- 4
- 5
- 6
- 7

Anterior diapositiva

6.

Confirma la operación

Revisa los datos y pulsa “Confirmar” para enviar la donación.

1.

Haz una donación

Ayuda en un par de clics desde CaixaBankNow, tu banca digital.

2.

Entra en Bizum

En CaixaBankNow, desde la pantalla principal pulsa “Bizum”. Después, selecciona la opción “Hacer donativo”.

3.

Selecciona el destinatario

Puedes hacer la donación tanto a un privado como a una organización.

4.

Escribe los dígitos de la ONG

Si envías dinero a una ONG, deberás introducir sus 5 dígitos.

5.

Introduce el importe

Deberás indicar un importe de entre 0,50€ y un máximo de 500€.

6.

Confirma la operación

Revisa los datos y pulsa “Confirmar” para enviar la donación.

1.

Haz una donación

Ayuda en un par de clics desde CaixaBankNow, tu banca digital.

Siguiente diapositiva

- 1
- 2
- 3
- 4

- 5
- 6

Anterior diapositiva

4.

Confirma la operación

Revisa los datos y pulsa “Confirmar” para realizar el pago.

1.

Paga tus compras online

Una forma fácil y segura de hacer compras desde CaixaBankNow, tu banca digital.

2.

Selecciona Bizum en la pasarela de pago

Cuando hagas una compra online, selecciona pagar con Bizum. Cuando lo hagas, Bizum te indicará cómo realizar el pago.

3.

Entra en CaixaBankNow

Al entrar, verás tu solicitud de pago pendiente. Pulsa “Acceder”.

4.

Confirma la operación

Revisa los datos y pulsa “Confirmar” para realizar el pago.

1.

Paga tus compras online

Una forma fácil y segura de hacer compras desde CaixaBankNow, tu banca digital.

Siguiente diapositiva

- 1
- 2

- 3
- 4



Actívalo en CaixaBankNow
Descarga la app y accede mediante este QR



Un Bizum... ¡y listo!

Preguntas frecuentes sobre Bizum

¿Cómo funciona?

Este servicio revolucionario permite realizar pagos inmediatos entre particulares con solo disponer de un móvil. Sin precargas y de forma segura.

El sistema Bizum no es una app independiente, sino que está integrada dentro de la app de **CaixaBankNow**.

Para poder enviar y recibir dinero, es necesario registrarse en el sistema Bizum a través de la app de **CaixaBankNow**.

1. Descarga la app de CaixaBank desde los stores de Google o Apple (compatible con iOS y Android 5.0 o superior).

2. Dirígete a "Operar" y selecciona la opción "Hacer un Bizum". Si no estás registrado, regístrate de forma rápida en dos sencillos pasos. Se te pedirá autenticación, para lo cual deberás utilizar tus tarjetas de coordenadas o la app de CaixaBank Sign.

3. Selecciona la acción que quieras realizar en "Enviar o solicitar dinero" y selecciona o introduce el número de contacto del destinatario.

4. Introduce el importe que quieras enviar y selecciona la cuenta desde la que harás el envío.

5. Finalmente, introduce el concepto y confirma la operación.

6. Si el destinatario está registrado, recibirá el dinero o la solicitud de forma inmediata. En caso contrario, podrás enviarle un aviso por SMS para que se registre.

7. Si el destinatario se registra en menos de 48 horas, el dinero se enviará inmediatamente (nunca se bloqueará el dinero previamente al registro del destinatario).

¿Hay límites de importe o de operaciones entre particulares?

Se han implementado una serie de límites operativos y de importe entre particulares para garantizar la seguridad del servicio. Podrás enviar desde 0,50 € hasta un máximo de 500 € por operación, con un límite de 2.000 € por día, y teniendo en cuenta que no podrás exceder un acumulado mensual de 5.000 €. Además, podrás recibir hasta 60 operaciones en un mes, por un importe máximo de 1.000 € por operación recibida, y un acumulado diario de hasta 2.000 € por NIF.

¿Hay límites de importe o de operaciones para compras con Bizum en comercios Online?

Podrás realizar compras de hasta 1.500 € por operación y por día. El importe máximo acumulado semanal y mensual es de 4.000 €.

¿Cuál es el importe máximo que puedo pagar con Bizum en Loterías y Apuestas del Estado?

Con Bizum puedes pagar apuestas por un importe de hasta 500 €/operación.

¿Cuál es el importe máximo que puedo cobrar con Bizum en Loterías y Apuestas del Estado?

Según la legislación vigente, solo podrás cobrar con Bizum los premios de hasta 2.000 €.

Consulta y gestiona los recibos

- Podrás devolver un recibo ya pagado.
- Fraccionar el pago.
- Cambiar la cuenta de cargo.
- Consultar el detalle.
- Consultar las órdenes de impago.

¡Fíjate en todo lo que puedes hacer!

Devolver un recibo ya pagado: podrán realizarse directamente y desde Banca digital CaixaBankNow las retrocesiones de recibos cargados siempre que estén dentro del plazo de devolución.

Dejar de pagar la domiciliación a partir del último recibo: no serán atendidos los pagos de los próximos recibos que presente la emisora seleccionada.

Fraccionar el pago con tu tarjeta de crédito:

El último recibo: podrás fraccionar el último recibo cargado en tu cuenta.

Los próximos recibos: a través de esta opción se fraccionarán los próximos recibos de la emisora seleccionada.

Cambiar la cuenta de cargo de la domiciliación.

Consultar el detalle de todos los recibos cargados, por compañías.

Consultar las órdenes de impago.

Con todas las ventajas de Banca digital CaixaBankNow:

Disponible las 24 horas del día, los 365 días del año.

Seguridad total, mediante tus claves de acceso personales.

Impresión inmediata del recibo.

¿Qué necesitas?

Ser titular del servicio de Banca digital CaixaBankNow y acceder a la operativa desde la pestaña "Cuentas", en la parte inferior de la pantalla.

Recuerda que necesitarás tener tu Tarjeta Banca digital CaixaBankNow a mano para poder autorizar las operaciones.

¿Lo sabías?

Puedes ahorrarte todo el papeleo [personalizando cómo recibir tu correo](#). Banca digital CaixaBankNow se encarga de tener tu archivo perfectamente actualizado y clasificado.

10 reglas para navegar de forma segura

1. Concienciación: cuando accedemos a Internet, tenemos que ser conscientes de los riesgos a los que nos exponemos. Es fundamental ser precavido con las páginas que visitamos y los archivos que descargamos.
2. Un buen antimalware: Un antimalware es un software que nos protege de código malicioso como virus, troyanos, ransomware, etc. Contar con un antimalware actualizado y bien configurado te evitará muchos problemas. Aun así recuerda que el antivirus no garantiza tu seguridad al 100%.
3. Actualizar el sistema operativo y aplicaciones: Tener correctamente actualizado el sistema operativo (Windows, Linux, Apple...) y todas las aplicaciones instaladas es una de las principales garantías para no dejar abiertas puertas de entrada a tu equipo que los ciberdelincuentes puedan explotar. Aunque la actualización de los equipos lleve su tiempo, y a veces haya que reiniciar, es fundamental para solucionar vulnerabilidades de seguridad del software instalado.
4. Utilizar contraseñas robustas: Es muy importante tener una contraseña muy robusta y diferente para cada tipo de uso (correo electrónico, redes sociales, banca electrónica...). ¿Algunos trucos? Que tengan más de 8 caracteres y combinen letras (mayúsculas y minúsculas), dígitos y caracteres especiales; evitar información personal como puede ser el DNI, nombres de familiares o conocidos y nunca utilizar patrones muy sencillos, ni palabras de diccionario. Para una mayor seguridad, se recomienda modificar periódicamente las contraseñas.
5. Gestor de contraseñas: Recordar muchas contraseñas es complicado. Por ello se recomienda utilizar un gestor de contraseñas que guarda las contraseñas de forma segura. Nunca deben anotarse las contraseñas en libretas o ficheros sin cifrar.
6. No acceder a sitios web de dudosa reputación: Para verificar la legitimidad de una página web, no basta con fijarse únicamente en si aparece un candado al lado de la dirección de la página web. Debes comprobar la legitimidad de su certificado digital, verificando que está

vigente y realmente ha sido emitido para la página web por la que queremos navegar.

7. Evitar descargas no conocidas: una de las mayores brechas de seguridad viene de la descarga de archivos. Si no estás totalmente seguro del origen de lo que estás descargando, evítalo o verifícalo antes de la descarga.
8. Redes WiFi gratuitas: Si utilizamos una red Wifi gratuita para navegar por páginas públicas, el riesgo es mínimo. No obstante, debemos evitar navegar por páginas web que nos piden la entrada de datos personales, como contraseñas o usuarios, ya que la Wifi podría estar comprometida y por tanto alguien podría interceptar nuestros datos personales. Debemos prestar la misma atención cuando nos conectamos a Wifis con contraseña conocida.
9. Cuida tu identidad digital: Toda la información que subimos a internet sobre nosotros mismos, las imágenes que compartimos en las redes sociales dejan un rastro digital que conforman lo que se conoce como nuestra ‘identidad digital’. Por ello, hay que vigilar especialmente con la ‘identidad digital’ que nos creamos y únicamente subir aquella información sobre nosotros mismos que consideramos cien por cien pública.
10. Desconfianza siempre activa: Aun teniendo los sistemas actualizados, un buen antivirus y prestando atención a todas las recomendaciones anteriores, el sentido común es lo más importante a la hora de navegar por internet. Recuerda que la mejor defensa eres siempre tú.

Nuevas tecnologías e internet. Un binomio prácticamente inseparable que nos hace estar constantemente **interconectados** con el ciberespacio. Este hecho no pasa desapercibido para los ciberdelincuentes, que buscan valerse del uso masivo e intensivo de internet como oportunidad para poder llevar a cabo sus ataques.

Para ayudar a sus clientes y a la sociedad en general, CaixaBank lleva a cabo diferentes **iniciativas** para dar a conocer los múltiples peligros digitales a los que se enfrentan los internautas y las **buenas prácticas digitales** que se pueden adoptar para **minimizar** el riesgo de ser víctimas de un ciberataque.

El factor humano, clave en los ciberataques

El factor humano es clave en los ciberataques. La clave del éxito de los ciberdelincuentes no pasa únicamente por el uso de tecnología cada vez más sofisticada, sino que, realmente el verdadero éxito son las técnicas de engaño que usan para poder llevar a cabo estos ataques, lo que llamamos la **ingeniería social**.

Aunque las herramientas informáticas de seguridad, como el antimalware, son **imprescindibles** para ayudar a **protegerse** ante un ciberataque, por sí solas **nunca son infalibles al 100%**. Otros aspectos como la permanente actualización de nuestros dispositivos y sus aplicaciones, una adecuada protección de nuestra identidad digital o el uso controlado de las conexiones wifi son igualmente importantes. Aun así, revisar con la [máxima atención](#) [cualquier mensaje](#) y no clicar en anexos o enlaces ante la más mínima sospecha; en definitiva, aplicar el sentido común, suponen sin duda nuestra mejor defensa. Por ello conviene estar al día de los **riesgos** a los que nos enfrentamos en nuestro día a día digital y **saber cómo evitarlos**.

CaixaBank y la cultura de ciberseguridad

Para CaixaBank, **la seguridad de las personas es lo primero**. Por este mismo motivo, lleva tiempo trabajando e implementando extensos contenidos y programas de concienciación sobre ciberseguridad para todos sus empleados, clientes y la sociedad en general.

Iniciativas como el boletín **CaixaBankProtect NEWS** que envía a sus clientes a través de email cada trimestre, la actualización permanente del [apartado de Seguridad de nuestra web](#), así como la difusión de contenidos en **redes sociales** o la participación y organización de **conferencias especializadas** marcan una **clara apuesta** de la entidad por la **cultura de seguridad**.

El *phishing* es una de las técnicas más usadas por los ciberdelincuentes para robar datos personales y bancarios. Con la ayuda de técnicas de [ingeniería social](#), el ciberdelincuente suplanta la identidad de entidades, personas, marcas o servicios conocidos para tratar de engañar a sus víctimas. Su objetivo final suele ser el dinero y/o la obtención de información sensible, generalmente introducida por la víctima en una página web falsa creada por el ciberdelincuente o infectando el equipo mediante la descarga de un *malware*.

A lo largo de los años, los *hackers* han evolucionado y perfeccionado sus métodos de engaño, creando correos *phishing* cada vez más sofisticados y difíciles de detectar. Por este motivo, para no caer en la trampa, el usuario debe aprender a reconocer las señales que puedan delatar al ciberdelincuente.

Cuando recibimos un nuevo correo, debemos formularnos las siguientes preguntas:

1. ¿El mensaje es sospechoso?

Para engañar a su víctima, el ciberdelincuente puede crear correos que inspiren confianza o curiosidad, suplantando la identidad de una entidad bancaria, de una plataforma de video en *streaming* o, simplemente, escribiendo un mensaje atractivo que impulse a clicar en un enlace o archivo anexo.

Aunque el remitente sea aparentemente conocido y/o el mensaje muy tentador, no se debe confiar en correos inesperados o en respuestas que no hayamos solicitado.

2. ¿Quién envía el correo?

Es imprescindible analizar con detalle la dirección de correo del remitente y no fiarnos solo del nombre que nos muestra. Debes fijarte siempre en el dominio que usa: si el correo es de una entidad o servicio, es muy probable que utilice sus propios dominios para las direcciones de email corporativas. Si recibes la comunicación desde un buzón de correo genérico tipo @gmail.com, @outlook.com o cualquier otro dominio no corporativo, empieza a sospechar.

Los ciberdelincuentes también pueden crear dominios que a simple vista parecen reales, pero en los cuales, si nos fijamos muy bien, podremos apreciar pequeñas modificaciones respecto del dominio real. Por ejemplo: caixabank.com es real, pero caixabanc.com, no lo es. Por ello, es necesario confirmar que la dirección de correo tiene el dominio oficial de la empresa y no dejarse engañar por pequeños cambios a veces casi imperceptibles.

Aun así, el dominio del correo se puede llegar a suplantar en su totalidad y los ciberdelincuentes pueden enviar correos electrónicos aparentemente desde la dirección legítima. Por este motivo es importante fijarse bien en el contenido del correo, tal y como se indica en los siguientes puntos.

3. ¿Es una petición urgente?

Crear sensación de urgencia es un recurso habitual entre los *hackers*. Mensajes como "Su contraseña ha caducado. Tiene 24 h para modificar sus claves de acceso..." empujan a la víctima a tomar una decisión rápida y precipitada.

Además de las prisas, el concepto de la confidencialidad también es muy usado en este tipo de estafas. Mensajes como "Por favor, no comentes esto con nadie más, es un asunto secreto y confidencial. Confío en ti..." pretenden disuadir a la víctima de realizar las comprobaciones de seguridad pertinentes y, por tanto, de no confirmar la petición con nadie más.

Por mucha urgencia o secretismo que transmita el mensaje, siempre se recomienda contactar con el remitente por un canal alternativo (por ejemplo,

llamando a los teléfonos habituales) para verificar que el correo es realmente legítimo.

4. ¿A quién va dirigido el correo?

Generalmente, las campañas de *phishing* son masivas y se dirigen a cientos de miles de personas en todo el mundo. Por lo tanto, es habitual que no cuenten con los datos personales de sus víctimas potenciales y usen términos genéricos como “amigo”, “Estimado cliente” o “Buenos días”, sin usar el nombre de pila de cada individuo.

Sin embargo, las técnicas de los *hackers* han ido perfeccionándose y cada vez son más numerosos los casos de *phishings* dirigidos y personalizados a víctimas concretas de las que previamente el ciberdelincuente ha obtenido información. Ejemplo de ello son las estafas del [fraude al CEO y el fraude facturas](#).

Por este motivo, que el remitente conozca el nombre del usuario no es una prueba de su legitimidad.

5. ¿El enlace es legítimo?

Si el correo contiene un enlace, es necesario comprobar a dónde conduce el mismo antes de clicar, ya que podría ser un enlace trampa. Debemos analizar su dirección web o URL para ver si es conocida. ¿Cómo?

Pasar el cursor por encima del enlace sin clicarlo permite ver la dirección web y comprobar si es o no conocida. Esta aparece en una pequeña ventana emergente y a los pies de la mayoría de los navegadores de Internet. Si la dirección a la cual dirige el enlace no corresponde a la que apunta el contenido del mensaje, podría ocultar una web maliciosa.

Es posible que algunos correos contengan enlaces más cortos de lo normal que no revelan información sobre su procedencia. En estos casos, es recomendable utilizar servicios gratuitos como los de <http://unshorten.it/>. Copiando y pegando el enlace acortado en esta web, se podrá saber la dirección completa y conocer dónde dirige realmente el enlace.

6. ¿Está bien escrito?

Que una entidad o compañía envíe una comunicación con una redacción y ortografía descuidadas es una señal de alarma que nos indica un posible correo fraudulento.

Las campañas de *phishing* en ocasiones se realizan desde el extranjero y están destinadas a atacar a personas de distintas nacionalidades. Por lo tanto, los ciberdelincuentes traducen sus mensajes a varios idiomas, en ocasiones

con muchos errores debido al uso de traductores automáticos.

Frases mal construidas, traducciones demasiado literales, palabras con símbolos extraños o fallos semánticos son pistas que pueden delatar a los estafadores. No obstante, cada vez son más habituales los casos de correos *phishing* elaborados con una escritura perfecta. Cualquier tipo de texto, esté bien escrito o no, es por tanto susceptible de ocultar un intento de fraude.

7. Si sigo sin estar 100% seguro...

Es posible que, aunque se analicen todos los elementos del correo, aún no puedas asegurar al 100 % su legitimidad. Los *phishings* son cada vez más sofisticados y en ocasiones es muy difícil distinguirlos de un correo legítimo.

En estos casos, debe confirmarse la autenticidad del remitente mediante otro canal. Es decir, si se recibe un correo sospechoso por parte de una empresa y/o persona, es conveniente ponerse en contacto por teléfono con las mismas para verificar que la comunicación es real y legítima.

¿Estás seguro que es CaixaBank quien te está contactando?

A pesar de que las empresas invierten cada día más en nuevas y mejores medidas de ciberseguridad, los usuarios debemos aprender a reconocer las amenazas que nos acechan en el mundo digital. Todos podemos ser objetivo de los ciberdelincuentes, incluidos los usuarios de servicios bancarios.

Por ejemplo, como usuario de [CaixaBank Sign](#), puedes recibir el correo o el mensaje de texto fraudulento de un ciberdelincuente con el asunto “tiene un problema con su CaixaBank Sign”.

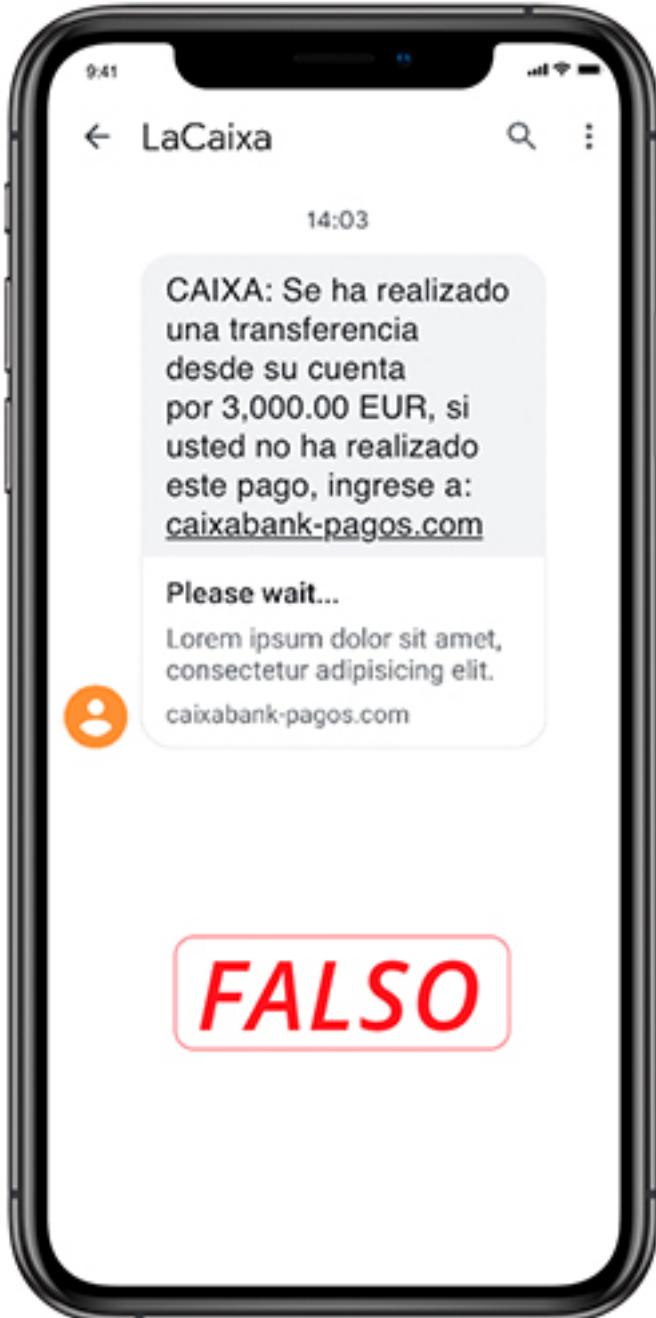
Si no analizas correctamente el correo siguiendo los anteriores pasos de seguridad, corres el riesgo de clicar en un enlace fraudulento, con lo que podrás llegar a ceder tus claves de acceso al ciberdelincuente.

En caso de duda, antes de clicar en cualquier enlace o fichero anexo, contacta con tu gestor de CaixaBank para asegurarte de que el correo es legítimo.

La palabra ***smishing*** proviene de la unión entre “SMS” y ***phishing***. Este tipo de estafa utiliza el envío de mensajes de texto o de mensajería instantánea tipo WhatsApp para engañarte y conseguir que realices alguna acción fraudulenta.

El objetivo del ciberdelincuente puede ser la obtención de tu información personal, la infección de tu dispositivo, o convencerte para que llames a algún número de teléfono de tarificación adicional, entre otros.

Para conseguirlo, al igual que con [los ataques de phishing por correo electrónico](#), los estafadores utilizan la ingeniería social para hacerte creer que has recibido una reclamación urgente por parte de tu banco, una oferta demasiado buena para ser cierta o el premio de algún concurso en el que no has ni participado.



¿Qué puedo hacer para evitar estos ataques?

- Desconfía de mensajes que traten de transmitir urgencia, que adviertan sobre algún tipo de riesgo sobre tu dinero o que te ofrezcan premios u ofertas especiales.

- Sé precavido con la información personal que compartes. Recuerda que **ni CaixaBank ni ninguna otra empresa o institución legítima te pedirá nunca las claves** de acceso de tu banca digital.
- **No hacer clic directamente en los enlaces de los SMS.** Si el mensaje contiene un enlace, analiza con detenimiento si la dirección web está bien escrita y si corresponde a la página oficial del servicio en cuestión. Si crees que el mensaje puede ser verdadero, es recomendable acceder a los enlaces **escribiendo la dirección directamente en la barra del navegador.**
- Es posible que algunos mensajes contengan **enlaces más cortos** de lo normal que no revelan información sobre su procedencia. En estos casos, es recomendable utilizar servicios gratuitos como los de <http://unshorten.it/>. Copiando y pegando el enlace acortado en esta web, **podrás saber la dirección completa** y conocer donde dirige realmente el enlace.
- **El sentido común y el conocimiento** son tu mayor aliado contra los ciberdelincuentes. Mantente informado sobre las últimas técnicas y modalidades de estafa para estar prevenido y mejorar tu seguridad digital.

Como detectar una estafa

¿Te podemos llamar desde el banco?

Sí, por infinidad de razones.

Algunos ejemplos de por qué te podemos llamar son:

- Citarte para una entrevista.
- Confirmar por seguridad si has realizado una operación desde tu banca online.
- Avisarte que tienes una tarjeta pendiente de recoger en la oficina.

¿Pueden hacerse pasar por un empleado de CaixaBank y llamarme?

Sí, las llamadas fraudulentas (vishing) están a la orden del día.

Los ciberdelincuentes sofistican cada vez más sus argumentos para engañar.

Algunas estrategias que utilizan son:

- **Suplantar el teléfono llamante** (Caller ID Spoofing) para que sea el mismo que el de nuestro centro de atención al cliente.
- **Conocer cómo funciona la banca electrónica** y por tanto guiarte por los menús para conseguir su objetivo.
- **Utilizar argumentos convincentes** como por ejemplo ayudarte a retroceder un supuesto cargo fraudulento.

¿Cómo van a intentar estafarme los ciberdelincuentes?

Es probable que **te pidan datos confidenciales**, como el número de tu tarjeta, tus claves de acceso a la banca online o bien, mediante diferentes pretextos como una supuesta retrocesión de un pago para que hagas tú el pago.

Es habitual que usen sistemas de pagos inmediatos como BIZUM o incluso que te pidan que hagas un reintegro con código a través de cajero automático.

¿En qué consiste la estafa del reintegro con código a través de cajero automático?

CaixaBank permite retirar dinero a través de un cajero automático mediante un código personal. Este servicio, que ofrece grandes ventajas para los clientes, es también un pretexto que usan los ciberdelincuentes para realizar estafas.

El pretexto suele ser que alguien está realizando un reintegro en un cajero y que, para anularlo, tienes que seguir los pasos que te indican. El ciberdelincuente, te guiará a través de tu banca online para conseguir que des de alta un nuevo reintegro y le facilites el código personal que te ha llegado para realizar el reintegro en un cajero.

El teléfono sigue siendo un canal muy utilizado por los estafadores para intentar engañar a posibles víctimas.

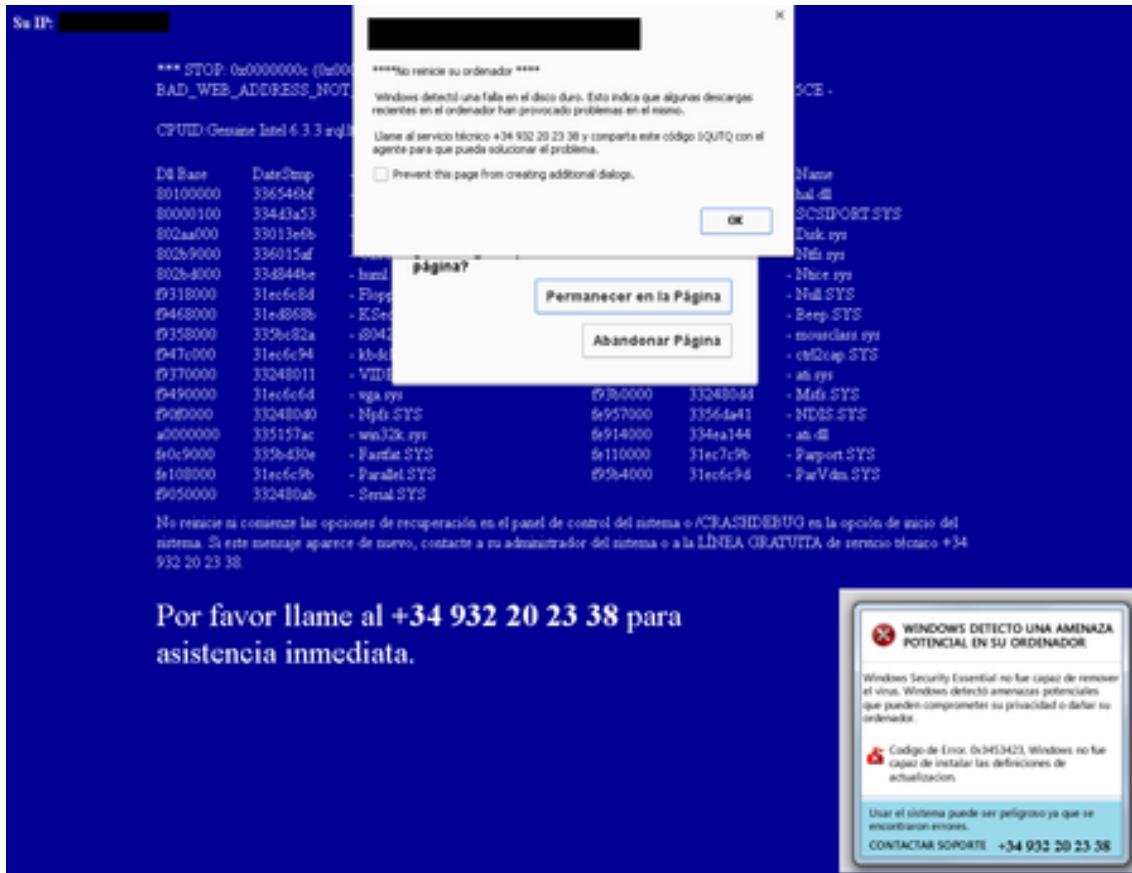
Este método de **estafa de ingeniería social**, también conocido como **vishing**, ofrece a los criminales la posibilidad de ser muy convincentes, ya que les permite mediante un argumento determinado ir adaptando su discurso en función de la respuesta de la víctima, para así poder dar mayor credibilidad a la llamada.

Uno de los pretextos más utilizados por los cibercriminales es el de **hacerse pasar por un técnico** de una importante empresa informática, para informar al usuario de que su ordenador sufre un incidente grave de seguridad y ofrecerle ayuda.

¿Cómo funciona este fraude?

El estafador se comunica con la víctima

Habitualmente es el estafador quien se comunica con la víctima mediante una llamada telefónica. Esta llamada puede darse desde teléfonos internacionales y el interlocutor puede ser de habla extranjera. No obstante, en ocasiones, es el usuario quien contacta con él al aparecerle una pantalla informando de un incidente grave con su ordenador mientras navega por internet, en el que se incluye un número de teléfono de contacto para solucionarlo.



El pretexto es el cebo para engañar a la víctima

El estafador informa a la víctima de que su ordenador tiene un incidente grave de seguridad y que pueden solventarlo simplemente siguiendo unas instrucciones y realizando un pago de una pequeña cantidad por los servicios prestados o bien en concepto de una suscripción por un tiempo determinado al soporte técnico de la compañía.

Instalación de un programa de control remoto

Para poder llevar a cabo las comprobaciones y la resolución de la incidencia, los estafadores instan a la víctima a instalar un programa de control remoto tanto en el ordenador como en el teléfono móvil. De esta manera, los delincuentes obtienen el control de los dispositivos.

Instalación de malware

En ocasiones instalan programas adicionales en el ordenador o teléfonos de las víctimas. Estos programas acostumbran a contener malware (código malicioso) que puede robar y/o dañar la información de los dispositivos.

Pago de los servicios prestados o por suscripción

Finalmente, los estafadores pedirán hacer el pago por los servicios prestados o por adherirse a una suscripción periódica al soporte técnico de la compañía.

Para hacer el pago, bien pueden pedir a la víctima que acceda a su banca online y ejecute una o diversas transferencias, o bien, pueden solicitar datos de una tarjeta bancaria para poder proceder al pago. Si la víctima procede a hacer una transferencia, los estafadores pueden modificar el importe antes de su emisión. En caso de que la víctima facilite los datos de su tarjeta bancaria, los estafadores harán operaciones en diversos comercios de internet.

¿Qué recomendaciones de seguridad se han de seguir para evitar ser víctimas de este tipo de fraude?

Usar el sentido común

Ante cualquier llamada telefónica no habitual y con un pretexto inesperado y que resulte extraño, se ha de desconfiar, usar **el sentido común** y no dar ningún dato, dando por finalizada la llamada.

Cuidado con instalar software desconocido

No se debe descargar e instalar ningún programa informático de fuentes desconocidas o a petición de un desconocido. Estos programas **pueden contener malware** que pueden dañar los dispositivos y la información que contienen.

Disponer de un antivirus y actualizaciones en regla

Se recomienda disponer siempre de un **antivirus**, así como tener el sistema operativo y aplicaciones actualizados a la última versión.

En caso de ser víctima, la rapidez es esencial

En caso de ser víctima de un caso de fraude telefónico, es esencial ponerlo en conocimiento lo más rápidamente posible de un gestor CaixaBank o al teléfono de atención 24h **93 887 25 25** o **900 40 40 90**.

Actúa con precaución. Ante cualquier duda, contacta con CaixaBank a través de los canales oficiales. Llámanos al 93 887 25 25 o al 900 40 40 90.

¿Qué es un deepfake?

Una técnica de inteligencia artificial

La tecnología deepfake es una técnica de inteligencia artificial que combina las palabras 'deep learning' (aprendizaje profundo) y 'fake' (falso).

Los deepfake son archivos de vídeo, imagen o voz manipulados mediante software de inteligencia artificial de modo que parezcan auténticos.

Son archivos de vídeo, imagen o voz manipulados con inteligencia artificial para que parezcan auténticos.

Los deepfakes suponen una amenaza porque pueden ser utilizados para perpetrar fraudes sofisticados. Por ejemplo, para simular un vídeo de un alto directivo o CEO anunciando noticias falsas o incluso causar fluctuaciones en el mercado de valores.

Por lo tanto, es crucial estar informado, ser crítico con el contenido multimedia que consumimos y saber cómo detectar un posible deepfake.

Cómo detectar un potencial deepfake

Detectar un deepfake no es sencillo, debido a la sofisticación de la tecnología, pero hay algunas señales que pueden ayudarnos a sospechar:

1. **Rostro y cuerpo:** Los deepfakes suelen centrarse en el rostro, por lo que si el cuerpo parece desproporcionado o mal alineado, es una señal para sospechar.
2. **Número de parpadeos:** Los deepfakes a menudo tienen dificultades para replicar el parpadeo natural de los ojos. Es decir, si en el vídeo el personaje no parpadea suficientemente, podría ser una indicación de falsedad del vídeo.
3. **Detalles faciales y de la piel:** En vídeos deepfake, los bordes de las imágenes pueden ser borrosos, la piel puede parecer demasiado lisa o arrugada y las expresiones faciales pueden ser entrecortadas o poco naturales.
4. **Verificación de fuentes:** Si un vídeo o cualquier contenido proviene de una fuente no verificada o poco fiable, debemos sospechar sobre su legitimidad.
5. **Extensión del vídeo:** Los deepfakes suelen ser vídeos cortos. Por tanto si el vídeo es largo, será más probable que sea legítimo.
6. **Software de detección de deepfakes:** Para procesos que requieren de una verificación más minuciosa, se puede recurrir a soluciones de detección de deepfakes. Cabe indicar que ninguna solución tecnológica va a poder garantizar al 100% la legitimidad o no de un vídeo.

Es importante recordar que ninguna de estas señales es definitiva por sí sola. La mejor defensa contra los deepfakes es una combinación de concienciación y cierto escepticismo, sentido común ante determinados contenidos y sobre todo revisar otras fuentes, antes de dar por buenos los mensajes que puedan aparecer en los vídeos.

Activa tu nueva firma

Hemos integrado la firma dentro de la app CaixaBankNow, tu banca digital. Actívala y elimina la app CaixaBank Sign.

Una nueva forma de firmar

Más comodidad

Podrás realizarlo todo desde la app **CaixaBankNow**, en la sección "Seguridad".

Menos aplicaciones

Ya no necesitarás la app CaixaBank Sign, podrás borrarla de tu móvil.

Máxima seguridad

Autoriza tus operaciones en cualquier lugar y con total seguridad.

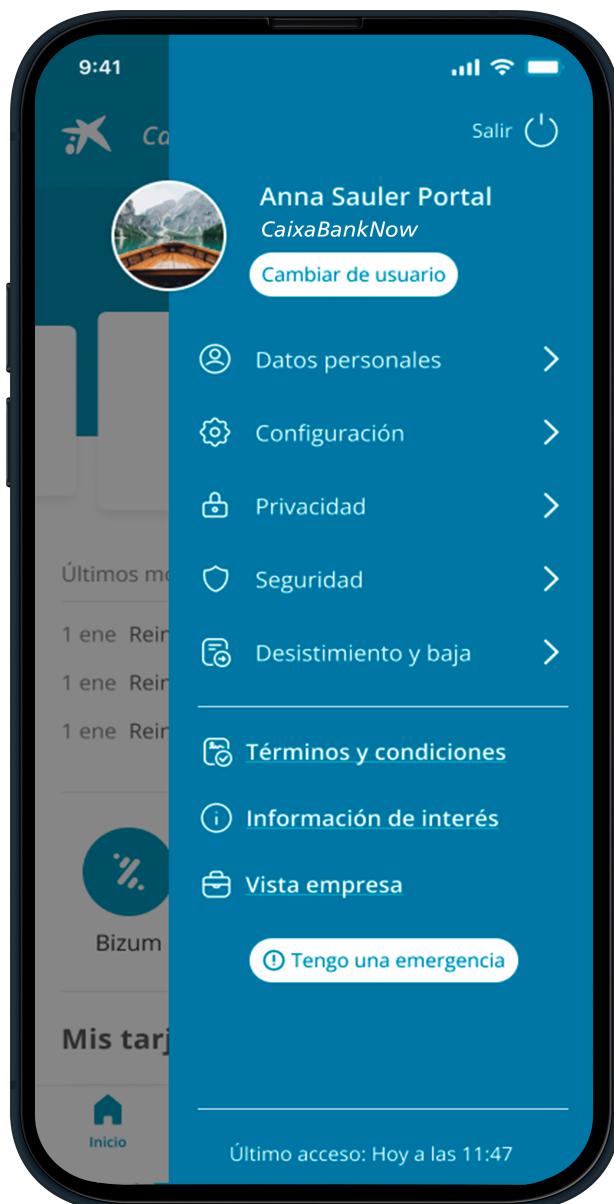
Comprueba que tienes instalada la última versión de CaixaBankNow y sigue estos pasos:

Entra en la app **CaixaBankNow**.

Accede a "**Perfil**", haz clic en "**Seguridad**" y, a continuación, en "**Firma**".

Activa tu nueva firma.

Elimina la app de CaixaBank Sign de tu móvil.



Preguntas frecuentes

No sé donde activar la firma

Entra en la app de CaixaBankNow con tus claves desde el dispositivo móvil donde quieras activar la firma y accede a "Perfil" > "Seguridad" > "Firma". Despues, selecciona la opción "Activar firma" y sigue las indicaciones.

Una vez hayas activado la firma, podrás borrar la app CaixaBank Sign. Si tienes varias claves de acceso (identificador y contraseña), tendrás que activar la firma para cada una de ellas.

¿Hasta cuándo puedo utilizar CaixaBank Sign?

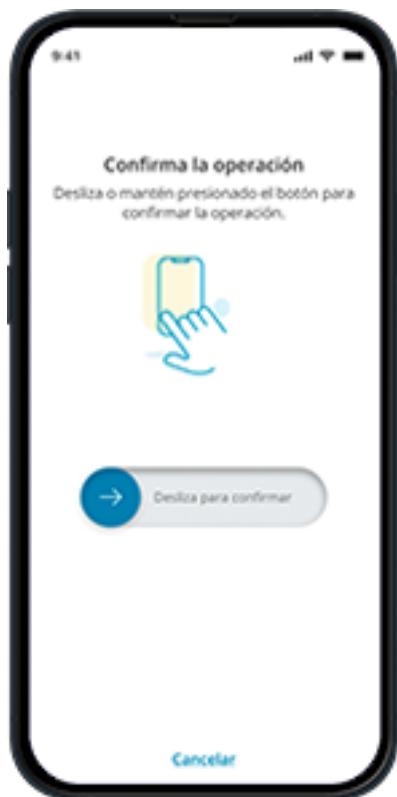
Durante un tiempo aún podrás seguir utilizando la app CaixaBank Sign, pero próximamente quedará obsoleta. Por ello, te recomendamos activar la firma en la app de CaixaBankNow lo más pronto posible y después borrar la app CaixaBank Sign de tu dispositivo.

¿Qué pasa si borro directamente la app?

Si borras directamente la app CaixaBank Sign, cuando vayas a realizar una operación en tu banca digital no podrás finalizarla. Es recomendable que actives tu firma dentro de la app CaixaBankNow para poder completar cualquier operación con normalidad.

¿Cómo firmaré cuando haya activado la firma?

Si estás realizando una operación en el mismo dispositivo donde tienes la firma activada, no tendrás que salir de la app para autorizar tus operaciones. Te pediremos que confirmes la operación deslizando tu dedo o manteniendo pulsado.



¿Puedo hacerlo desde el ordenador?

No, por motivos de seguridad, únicamente puedes activar la firma en dispositivos móviles.

Si inicias una operación desde el ordenador, te pediremos que la confirmes desde tu dispositivo de firma.

¿Puedo activar la firma en dos móviles diferentes?

Puedes tener la firma activada en un solo dispositivo. Si has cambiado de dispositivo móvil o quieres activarla en otro dispositivo diferente al actual, tendrás que abrir la app CaixaBankNow, acceder a "Perfil > "Seguridad" > "Firma" y seleccionar la opción "Activar firma en este dispositivo".

Si activas la firma en un nuevo dispositivo, se desactivará la firma del dispositivo anterior.

Descubre el modus operandi de los ciberdelincuentes y evita caer en la trampa

La estafa del like consiste en **engañar a los usuarios ofreciendo falsas ofertas de trabajo** que consisten en dar likes a anuncios o vídeos o en seguir a un perfil determinado.

Fin del fraude

La cantidad de dinero a invertir aumenta progresivamente hasta que, en un momento dado, **el reembolso prometido no es abonado y se corta todo** contacto con la víctima.

Contacto inicial

Los estafadores contactan a sus víctimas de forma aleatoria **a través de aplicaciones de mensajería instantánea**, ofreciéndoles una remuneración a cambio de incrementar los seguidores, dar "me gusta" a vídeos o anuncios o realizar tareas en aplicaciones relacionadas con criptomonedas.

Generación de confianza

Para generar confianza, las víctimas **reciben una pequeña compensación por las primeras tareas realizadas**. Este pago inicial sirve para **aportar credibilidad y legitimidad** al supuesto trabajo.

Escalamiento del fraude

Después de recibir el primer pago, **las víctimas son agregadas a un chat grupal** con la persona que publica las tareas, otras víctimas y bots. Los bots simulan usuarios reales y **publican capturas de pantalla falsas mostrando supuestas ganancias**.

Incremento de la dificultad

Las tareas se vuelven progresivamente más complejas y con mayores recompensas. Ahora, solicitan el **envío de dinero a destinatarios desconocidos** con la promesa de devolución y una bonificación adicional.

Fin del fraude

La cantidad de dinero a invertir aumenta progresivamente hasta que, en un momento dado, **el reembolso prometido no es abonado y se corta todo** contacto con la víctima.

Contacto inicial

Los estafadores contactan a sus víctimas de forma aleatoria **a través de aplicaciones de mensajería instantánea**, ofreciéndoles una remuneración a cambio de incrementar los seguidores, dar "me gusta" a vídeos o anuncios o realizar tareas en aplicaciones relacionadas con criptomonedas.

Protégete en 3 pasos

1. Desconfía de las ofertas demasiado buenas

Los trabajos que prometen altas remuneraciones por tareas sencillas suelen ser fraudulentos.

2. Verifica la identidad

Antes de compartir información o realizar pagos, asegúrate de verificar la identidad de quien te contacta. No confíes en perfiles desconocidos.

3. No facilites datos personales o bancarios

Nunca compartas tus datos personales o bancarios con personas o empresas que no conoces.

Si crees que puedes ser víctima de una estafa, contacta con nosotros cuanto antes

Teléfono de atención al cliente 24 h

900 40 40 90

Teléfono de atención al cliente desde el extranjero

+34 938 87 25 25

Conoce qué tipo de cookies existen y si es legal pagar por navegar sin ellas

Cuando navegamos por internet, es común encontrarnos con ventanas emergentes solicitando la aceptación de cookies o el pago de una suscripción para navegar sin ellas. Pero, **¿qué significa realmente aceptar o rechazar cookies?**

¿Qué son las cookies?

Son **datos almacenados en tu navegador** cuando visitas una página web. Contienen información sobre tus preferencias de navegación, configuraciones, datos de inicio de sesión y productos guardados en tu lista de favoritos.

¿Para qué las necesitamos?

Permiten **recordar datos** de inicio de sesión, ajustes de idioma y ubicación, y guardar productos en la cesta de la compra. Además, **recopilan datos sobre cómo interactuamos** con un sitio web para mejorar su rendimiento.

¿Quién las gestiona?

- **Cookies propias:** son **generadas por el sitio web** que estás visitando y se utilizan internamente para mejorar la experiencia del usuario (recordar tu inicio de sesión, tus productos en la cesta de la compra...).
- **Cookies de terceros:** crean perfiles de usuario **para enviar publicidad personalizada**, así los anunciantes pueden rastrear tu actividad en diferentes sitios web.

¿Qué tipo de cookies existen?

Los tipos más habituales son:

- **Técnicas:** esenciales para la operativa básica del sitio web.
- **Funcionales:** evalúan qué, cómo y cuándo se utilizan las funciones del sitio web.
- **De preferencias:** recuerdan tus ajustes personales, como el idioma o la región.
- **De análisis:** analizan el comportamiento del usuario para mejorar el servicio.
- **De publicidad comportamental:** crean perfiles de usuario para mostrar anuncios personalizados.
- **De sesión:** se activan mientras visitas la web y se eliminan al cerrar el navegador.
- **Persistentes:** guardan, acceden y tratan los datos durante un tiempo establecido.

Pagar por rechazar cookies: ¿es legal?

Según la Guía de 2024 de la Agencia Española de Protección de Datos (AEPD), **es legal ofrecer la opción de pagar para navegar sin cookies**. No se puede impedir a los usuarios acceder al servicio si rechazan las cookies, pero la alternativa al rastreo puede no ser gratuita.

Qué es mejor, ¿rechazar o aceptar las cookies?

Rechazar cookies y pagar por la privacidad: ofrece **mayor privacidad** a cambio de un coste mensual. Sin embargo, será **menos personalizada** y no garantiza una navegación totalmente anónima, ya que existen otras formas de seguimiento.

Aceptar cookies y navegar gratis: implica ceder tus datos de navegación a cambio de acceso gratuito al contenido. Aunque no hay un pago directo, pagas con tus datos personales y te expones a anuncios personalizados.

¿Por qué es tan importante informar de una pérdida o robo del móvil?

El móvil se ha convertido actualmente en una herramienta más de trabajo y también en **otra manera de almacenar toda nuestra información** (fotografías, notas, etc.), **hacer pagos o acceder a nuestras cuentas bancarios**. El robo o la pérdida de tu smartphone puede causar **consecuencias negativas**, por la pérdida material y por el mal uso que pueden hacer los ladrones si el dispositivo no ha sido protegido correctamente.

Por este motivo, **es de vital importancia que, en el mismo momento que detectes el robo o la pérdida de tu dispositivo móvil, lo comuniques a la entidad bancaria para que pueda tomar las medidas preventivas necesarias**, como por ejemplo el bloqueo del acceso a la banca en línea o a las tarjetas bancarias. **Si tu entidad bancaria es CaixaBank, te puedes poner en contacto a través del teléfono 24 horas 900 40 40 90 o +34 93 887 25 25.** También puedes revisar estos consejos para [mejorar la seguridad de tu smartphone](#).

¿Cuáles son los riesgos de perder el móvil?

Intentos de chantaje o extorsión

Si el teléfono móvil carece de protección o dispone de alguna muy débil, los ladrones tendrán acceso a todos los datos almacenados en él, como fotografías, correos electrónicos, mensajes de texto, acceso a las redes sociales o a cualquier otro tipo de información relevante que tengamos almacenada. Con toda esta información, los delincuentes pueden realizar suplantaciones de identidad o solicitar una compensación económica para que estos datos no sean expuestos públicamente.

Intentos de acceso a la información y apps de tu móvil

Si tienen acceso a tu móvil, es posible que intenten acceder también a la información o apps que hay en él, incluso a tu banca *online*. Aunque para acceder a tu banca online necesitarán el patrón, PIN o biometría de desbloqueo de tu dispositivo, y además las credenciales de acceso a la app de tu entidad bancaria.

¿Cuáles son los riesgos de perder tu documento de identidad?

Los **documentos de identidad** (pasaporte, DNI o tarjeta de residencia) son **documentos oficiales que contienen datos de identificación personal** de cada uno de sus titulares.

La **pérdida o robo** de estos documentos conlleva un **alto riesgo**, puesto que la persona que se apodere de ellos podría utilizarlos de forma malintencionada **suplantando la identidad del titular** y actuando en su nombre, por ejemplo, para conseguir información confidencial, reintegrar importes desde cuentas bancarias, contratar préstamos, entre otros.

Por ello, ante esta situación, **es muy importante actuar rápidamente**.

¿Qué hacer si extravías o te roban el documento de identidad?

Interpón una denuncia policial

Si pierdes o te han robado tu documento de identidad, el paso más importante es realizar una denuncia policial, que te servirá para **protegerte ante cualquier intento de suplantación de identidad**.

Comunícalo a tu entidad bancaria

Las entidades bancarias deben ser conocedoras de la pérdida o robo del DNI para que puedan aplicar las medidas correspondientes y proteger a sus clientes. Si tu entidad bancaria es CaixaBank, puedes ponerte en contacto a través del **teléfono 24 horas 900 40 40 90 o +34 93 887 25 25**.

Internet te permite ir al supermercado, renovar el armario o reservar tus próximas vacaciones desde la comodidad del hogar. Por este motivo, cada día más usuarios deciden realizar sus compras online. El comercio electrónico es cómodo y práctico, y aplicando las medidas de protección adecuadas, **también seguro**.

Si deseas comprar en tiendas online con tu tarjeta, en CaixaBank deberás confirmar la orden de pago mediante **CaixaBankNow** como último paso. Cuando recibas el mensaje en la app, **no te precipites. Revisa con atención que los datos de la compra son correctos, especialmente el comercio y el importe**. Tienes unos minutos para hacerlo. Ante cualquier duda, cancela la operación.

Adicionalmente, para no caer en engaños y proteger tu dinero y tus datos, sigue las siguientes claves para hacer tus compras online:

- **Cuidado con las superofertas y los enlaces**

Es posible que recibas muchas ofertas comerciales en tu buzón de correo o por cualquier otro canal, algunas anunciando precios muy por debajo de los de la competencia. **Si una oferta parece demasiado buena para ser cierta, sospecha.** Los precios anormalmente bajos pueden ser una trampa para atraer a compradores incautos. También desconfía si expira en poco tiempo. Es una forma de animarnos a caer en la trampa, pues quieren que vayamos con prisas para que no analicemos detenidamente la propuesta. Indaga otras webs y otros distribuidores para confirmar el valor real de mercado del artículo. Además de desconfiar de correos sospechosos, debes tener cuidado con las ofertas que te lleguen por otros canales, como mensajes de WhatsApp o ventanas emergentes o incluso llamadas telefónicas. Aunque puedan ser de tu interés, **tómate unos instantes para analizar la legitimidad del vendedor antes de comprar o abrir los enlaces o adjuntos que puedan contener.**

- **Webs legítimas**

Aunque las páginas **web tengan un candado y empiecen por HTTPS://, no significa que sean legítimas.** Solo nos indica que la información viaja cifrada desde tu dispositivo hasta la web gracias a un certificado. Los ciberdelincuentes pueden conseguir estos certificados con facilidad. Por lo tanto, el hecho de que una web empiece por HTTPS, o lo que es lo mismo, tenga un candado, no supone ninguna garantía de validez.

Por ello es muy **importante fijarse detalladamente en qué página web estamos** realmente. Además, para comprobar si el certificado digital está en vigor y si corresponde realmente al de la web a la que quieras acceder, puedes clicar en el candado y ver información más detallada.

- **Conexiones seguras**

Recuerda **no utilizar nunca una conexión pública para realizar tus compras online**, ya que no ofrecen ninguna garantía de seguridad. Siempre que debas introducir datos bancarios o personales para realizar transacciones, asegúrate de hacerlo a través de una red WiFi privada y segura.

- **Aspecto de la web**

Si estamos atentos, es probable que el aspecto general de la web nos dé pistas sobre su legitimidad. Debemos **fijarnos detalladamente en el enlace y revisar si es correcto.** A veces, el cambio de una sola letra a otra similar es suficiente para engañarnos. Además, algunas webs fraudulentas cometan una serie de errores de diseño que las delatan: varios tipos de letra en la misma página, imágenes de baja calidad, textos mal traducidos, entre otros detalles.

- **No tengas prisa por confirmar el pago con la app**

Cuando quieras pagar en una tienda online con tu tarjeta, el sistema te

pedirá que confirmes el pago mediante **CaixaBankNow**. Recibirás un mensaje en la app con los detalles de la operación, indicando el nombre de la tienda y el importe. **Antes de aceptar cualquier operación, revisa que todos estos datos son correctos y que corresponden a tu compra.** Si hay algo que no te cuadra, cancela la operación.

- **Opiniones de otros usuarios**

Ya sea porque sospechas de la veracidad de la tienda, o porque debes escoger entre varias opciones, es recomendable realizar una búsqueda previa para **encontrar referencias de otros usuarios**. Es posible que otros compradores hayan compartido su experiencia en internet y puedan ayudarte a escoger la opción más segura o la que más se adapte a ti.

- **Revisa tus cuentas**

Revisar periódicamente el estado de tus tarjetas y tus cuentas es una buena medida de seguridad para compradores online. **Comprueba que todos los movimientos han sido realizados por ti**, especialmente después de realizar algún pago por comercio electrónico. Si tienes alguna duda o sospecha, contacta con tu oficina bancaria. Finalmente, **activa las notificaciones de tu app bancaria** para que te avise de cualquier gasto, aunque sea mínimo, y así no se te escape nada que pueda llegar a ser anómalo.

- **Una tarjeta para las compras online**

Para evitar algunas sorpresas, **dedica una única tarjeta a las compras que hagas por Internet con un saldo ajustado** a cada compra por ti mismo.

En definitiva, no caer en las trampas de los ciberdelincuentes depende esencialmente de nosotros, de ser precavidos y de aplicar mucho sentido común y, por supuesto, no dejarse llevar por las prisas.

Consejos para crear una contraseña segura y qué hacer frente a un posible compromiso

Las contraseñas son la llave que abren la puerta a tu mundo digital. La seguridad de tus cuentas, datos personales, información bancaria y personal dependen, en gran medida, de la calidad y la robustez de las contraseñas de acceso que utilices. **Por eso es vital que, como usuario, sepas crear contraseñas robustas.**

La receta para una contraseña perfecta

Utiliza una contraseña larga que contenga números, letras y símbolos

- Como mínimo debe tener 8 caracteres combinando números, letras y símbolos. Cuanto más larga sea, más difícil será de averiguar.
- Puedes probar con la letra de una canción, un nombre de un libro o alguna frase que signifique algo para ti y que solo tú recuerdes.

Evita utilizar datos personales o palabras comunes

- El nombre de tu perro, la fecha de tu boda o el día en que naciste serán los primeros códigos que los ciberdelincuentes introducirán para tratar de acceder a tus cuentas.

No utilices una única contraseña

- ¿Qué pasaría si perdieras una llave maestra que abriera a la vez tu casa, tu vehículo, tu buzón de correo y tu oficina? Si utilizas solo una contraseña, estás corriendo el mismo riesgo. Si comprometen la contraseña que reutilizas para todas tus cuentas, tu mundo virtual estará en peligro. Utiliza una distinta para cada cuenta.

Utiliza un gestor de contraseñas

- Puedes usar un gestor de contraseñas si tienes muchas y te es difícil poder recordarlas todas. Antes, asegúrate de consultar la fiabilidad y reputación de la herramienta que utilizarás.
- Nunca escribas tus contraseñas en libretas, tarjetas, ficheros, etc
- Evita guardar las contraseñas en el navegador. Utiliza un gestor de contraseñas.

Hoy en día el teléfono móvil es una **pequeña gran puerta de entrada a todo nuestro mundo digital**. Con él podemos acceder a nuestra información más sensible y confidencial, tanto financiera como personal. Los ciberdelincuentes lo saben y por ello dirigen sus ataques también hacia estos dispositivos. Es importante aprender a aumentar su seguridad con estos simples consejos:

Activa el bloqueo automático

Protegiendo el acceso con mecanismos de bloqueo automáticos, ayudarás a **mantener tu móvil más seguro cuando tú no lo estés usando**. Además, si pierdes el teléfono, esta medida impedirá que personas ajenas tengan acceso a la

información que contiene. Puedes **utilizar un patrón, un PIN y/o configurar el reconocimiento biométrico** para los dispositivos que lo permitan.

Mantenlo actualizado

Es indispensable que el sistema operativo de tu smartphone, sea Android o iOS, **esté actualizado con la última versión disponible para evitar y corregir vulnerabilidades de seguridad**. Para que no te olvides de hacerlo, puedes **configurar la actualización automática** de instalación nuevas versiones. Esta recomendación no solo aplica al sistema operativo, sino **también a todas las apps** instaladas en tu móvil.

Instala un antimalware

A veces olvidamos que un smartphone es como un pequeño ordenador de bolsillo y que puede sufrir los mismos ciberataques como cualquier otro dispositivo. Para prevenirlo, es recomendable que instales y mantengas actualizado **un antimalware para proteger tu información personal y confidencial**.

Antes de instalar una app...

Asegúrate de hacerlo desde las tiendas oficiales: Play Store para Android, App Store para iOS y AppGallery para Huawei, aunque esto no quiere decir que todas las apps disponibles a través de estas tiendas sean seguras o adecuadas para tu privacidad. Debes **prestar atención a los términos y condiciones que solicita cada app**, y valorar si están justificados o son excesivos para las funcionalidades que ofrece la app.

[Aquí](#) puedes consultar todo lo que debes tener en cuenta antes de instalar cualquier app.

Ten precaución si te conectas a redes de WiFi abiertas

En el aeropuerto, en el hotel, en el bar o en la calle... Cada día es más fácil encontrar redes WiFi públicas que permiten a cualquier usuario conectarse a internet.

Aunque puedan sacarte de un apuro si no tienes datos en tu móvil, hay que tomar ciertas precauciones: Por ejemplo, si decides utilizarlas, **evita acceder a servicios en los que tengas que introducir tus datos personales o confidenciales** (banca *online*, compras por internet, acceso al *email*, etc.). Las redes WiFi públicas podrían estar comprometidas y, por tanto, tus datos podrían ser interceptados por los ciberdelincuentes.

Realiza copias de seguridad

Además de servirte para recuperar tu información en caso de pérdida o robo del móvil, también estarás protegiendo todos tus datos ante infecciones de *malware* (especialmente las de *ransomware*, que cifran el contenido de los ficheros y te piden un rescate en *bitcoins* si quieres recuperar la información).

Con tu copia de seguridad, este “secuestro” de tu información no te arruinará el día, ya que tendrás tu información asegurada en otro dispositivo o en la nube.

¿Y si lo pierdes o te lo roban?

Si has seguido el primer consejo, aplicando un bloqueo de acceso en tu móvil como un patrón o PIN e incluso un reconocimiento biométrico adicional, será más difícil que cualquier persona acceda a tu dispositivo y a la información que contiene. Aun así, **es recomendable que lo bloqueeas a distancia**.

Para hacerlo, es importante **que sepas cual es el número del IMEI de tu dispositivo**: Con este número puedes pedir el bloqueo de tu móvil a tu operador, además de que te facilitará el poder poner una denuncia ante la policía.

Consulta [aquí](#) cómo actuar.

5 consejos que aumentarán la seguridad de tus dispositivos

Ordenadores, tabletas y teléfonos inteligentes: dispositivos con distinto aspecto, tamaño y funcionalidad. Ya conoces sus diferencias, pero **¿sabes qué tienen en común? Que requieren las mismas medidas de seguridad para estar protegidos**. Si quieras aumentar la seguridad de tus dispositivos, aplica estas medidas en todos ellos:

1. **Protege el acceso**

No todo el mundo debería poder entrar en tus dispositivos. Protege el acceso con mecanismos seguros de desbloqueo. Por ejemplo, puedes utilizar una contraseña robusta para acceder al ordenador, un patrón, PIN y/o configurar el reconocimiento biométrico para los dispositivos que lo permitan. Aplica, además, un bloqueo automático en caso de inactividad prolongada por tu parte.

2. **Comprueba que estén actualizados**

Es indispensable que el sistema operativo con el que funciona tu dispositivo esté actualizado con la última versión disponible. Por tanto, debes configurar la actualización automática de nuevas versiones y aceptarlas en cuanto tu dispositivo te avise de ello.

3. **El antivirus no es solo para el ordenador**

Muchos usuarios aún creen que los antivirus solo pueden o deben usarse en el ordenador. La realidad es que también son necesarios para móviles y tabletas, ¿o acaso estos últimos no se conectan a internet y pueden sufrir ciberataques?

Hay muchas opciones de antivirus, tanto de pago como gratuitas. Haz una búsqueda y encuentra el más adecuado para tu dispositivo.

4. **Descarga solo aplicaciones seguras y revisa los permisos**

Antes de descargar alguna de los miles de aplicaciones disponibles que existen en alguno de tus dispositivos, asegúrate de hacerlo mediante los canales oficiales de cada sistema operativo.

Pero cuidado, no todas las apps son seguras. Hay algunas que, aunque no contengan ningún elemento malicioso, pueden poner en riesgo tu privacidad. Por eso debes revisar los permisos que te piden antes de su instalación. Por ejemplo, ¿tiene sentido que una app de linterna para el móvil te pida acceso a tus fotos? Utiliza el sentido común y si te piden

permisos excesivos revisa si hay otras opciones menos intrusivas.

5. **Haz copias de seguridad**

Seguro que, como muchos, en algún momento has perdido o te han robado algún dispositivo. Si esto llega a pasarte, desearás haber hecho copias de seguridad de tu dispositivo. Puedes perder el móvil, el ordenador o la tableta, pero vas a poder recuperar la información que contienen. Adicionalmente estarás protegido ante infecciones por malware, especialmente el ransomware, que cifra el contenido de todos los ficheros pidiendo un rescate en bitcoins.

Tu seguridad también se incrementa en las compras presenciales *contactless* que realizas

La Directiva Europea de Servicios de Pago (PSD2) incrementa la seguridad en las compras presenciales *contactless*.

La PSD2 establece que se debe introducir el número secreto PIN¹ con más frecuencia en las compras presenciales *contactless*² para verificar la identidad de quien realiza el pago.

Tras aproximar tu tarjeta al terminal de pago (datáfono) del comercio para realizar la compra, solo tienes que seguir las instrucciones que aparecen en la pantalla del terminal:

En otros casos solo se indicará que teclees el número secreto PIN, sin necesidad de introducir la tarjeta.

En algunos casos se indicará que introduzcas la tarjeta en el terminal y teclees el número secreto PIN.

Cuando hagas compras con tu dispositivo móvil no será necesario introducir el número secreto PIN, porque tu identidad ya habrá sido verificada previamente³.

¿Qué debo hacer si he olvidado o bloqueado el número secreto PIN de mi tarjeta?

Si no recuerdas tu número secreto PIN, puedes obtener uno nuevo:

En un cajero CaixaBank
("Otras opciones" > "Cambiar PIN")

En una oficina CaixaBank

O puedes llamar al teléfono de asistencia:
+34 938 87 25 25 / +34 900 40 40 90

Si lo has bloqueado, al haber superado el máximo de tres intentos para introducir correctamente el número secreto PIN de tu tarjeta, puedes desbloquearlo:

En CaixaBankNow: al bloquear el PIN recibes en tu dispositivo móvil un SMS o una notificación para poder desbloquearlo en CaixaBankNow.
También puedes desbloquearlo desde el menú de la tarjeta en CaixaBankNow.

En una oficina CaixaBank

O en el teléfono de asistencia: **+34 938 87 25 25 / +34 900 40 40 90**

PSD2 ¿Cómo te afecta?

Recientemente han entrado en vigor un conjunto de normas (PSD2) que mejoran tus derechos como consumidor incrementando la seguridad en tu banca digital CaixaBankNow y en tus tarjetas emitidas por Payments&Consumer o M2P.

+ Protección

de la información de tus cuentas y tarjetas

+ Seguridad

en tus operaciones de pagos y compras

1. Tu identidad es lo más importante

Reforzamos la seguridad en el acceso a tus cuentas a través de CaixaBankNow, móvil o web. También en los pagos que puedas hacer desde esos entornos y en las compras con tarjetas por internet.

¿Cómo lo vamos a hacer?

Te pediremos que confirmes tu identidad a través de alguno de los siguientes métodos que, cuando operes en CaixaBankNow o con tus tarjetas, se combinarán con tu contraseña:

Firma con CaixaBank Sign...

... con la tarjeta de coordenadas...

... o a través de un SMS.

¿Cuándo lo vamos a hacer?

- Cuando accedas a CaixaBankNow, desde un dispositivo (teléfono móvil, navegador web) no asociado a tu perfil.
- Cuando realices pagos a través de CaixaBankNow.
 - Si firmas con la app CaixaBank Sign: te solicitaremos adicionalmente tu contraseña de acceso (PIN1) a CaixaBankNow.
 - Si firmas con tarjeta de coordenadas: te solicitaremos una clave adicional enviada por SMS.
 - Si firmas con claves SMS (cliente ImaginBank): te solicitaremos repetir tu contraseña (PIN1) de acceso.
- Cuando realices compras con tarjetas en comercios electrónicos. En estos casos, recibirás con más frecuencia el SMS con el código para confirmar tu identidad.
- Cuando hayas realizado varias compras seguidas con tu tarjeta en dispositivos contactless sin introducir el PIN, es posible que el TPV te indique en la siguiente compra que introduzcas tu tarjeta y teclees el PIN.

2. Cuando hablamos de seguridad, tú también tienes un papel relevante

La experiencia nos ha enseñado que si sigues unos sencillos consejos, puedes mejorar tu seguridad. Como expertos en la materia, vamos a ayudarte.

Enviaremos a tu correo electrónico, de forma periódica, una *newsletter* con consejos, información sobre novedades y noticias de seguridad para que estés siempre informado.

Toda esta información podrás consultarla en el apartado de seguridad de la web de particulares de Caixabank.

También podremos remitirte **alertas de seguridad por SMS** si detectamos que se realizan operaciones inusuales desde tu banca digital o tus tarjetas.

3. Queremos que nunca pierdas el control

Te informaremos de las situaciones que pueden afectar al funcionamiento de tu banca digital CaixaBankNow o de tus tarjetas a través del canal de comunicación que consideremos más idóneo para que puedas adoptar medidas a tiempo y evitarte perjuicios y molestias (sms, correo electrónico, notificaciones push, etc).

Dispones de la posibilidad de limitar operativas de tus tarjetas, como reintegros en efectivo en cajeros, compras en internet o en determinados sectores de actividad, para adaptar las condiciones de uso de la tarjeta a tus necesidades. También puedes bloquear temporalmente tus tarjetas. Puedes acceder a estas funcionalidades desde *CaixaBankNow/tarjetas/Consultas y gestiones/ opciones: Caixabank protect-Control de uso o bloquear tarjetas*.

4. Necesitamos tu número de teléfono móvil y tu correo electrónico actualizados

Tu teléfono móvil y tu dirección de correo electrónico van a ser necesarios para que puedas seguir operando con tu banca digital CaixaBankNow o con tus tarjetas.

Puedes actualizar estos datos sin moverte de casa: accede a la banca digital CaixabankNow, busca el apartado configuración en la parte superior derecha, accede a “modificar mis datos personales”, luego a “modificar teléfonos” o “modificar correo electrónico” y añade o modifica el tuyo.

También puedes actualizarlo acudiendo a tu oficina.

Nuevos Derechos

La nueva normativa te concede nuevos derechos, como por ejemplo:

- Derecho de devolución incondicional de recibos durante las primeras 8 semanas desde su adeudo en cuentas.
- Derecho a obtener una respuesta a las reclamaciones que puedas plantear ante el Servicio de Atención al Cliente en un plazo máximo de 15 días hábiles, prorrogable hasta un mes en casos excepcionales y siempre que te comuniquemos el motivo de la prórroga

Más derechos con PSD2

La nueva normativa de servicios de pagos te otorga:

- **Más seguridad en tus operaciones de pago:** tal y como te hemos explicado en el apartado de [PSD2: ¿cómo te afecta?](#), a partir del 14 de septiembre se ha reforzado la seguridad en el acceso a tu banca electrónica y en todas las operaciones de pago.
- **Más transparencia:** la información sobre los productos y paquetes de productos se presentará de manera clara e informando de su adquisición separada, así como de los costes y comisiones asociadas a cada producto o servicio. Además, las entidades bancarias están obligadas a remitir al Banco de España información sobre los servicios más comunes y las comisiones asociadas a estos. Se prevé en un futuro que el sitio web del Banco de España permita comparar estas comisiones.
- **Más facultades:** en cuanto a los adeudos domiciliados (recibos), podrás rescindir la autorización para su cargo en tu cuenta hasta que esta sea recibida por tu banco. Además, si no estás de acuerdo con un cargo en tu cuenta, podrás solicitar su devolución de manera incondicional durante las 8 primeras semanas desde su cargo. Además, si consideras que una operación en tu cuenta no la has autorizado tú, podrás solicitar su devolución durante los 13 meses siguientes a su cargo, te abonaremos su

importe y se analizará si estaba autenticada. En caso de no estarlo, se confirmará la devolución del importe.

- **Más libertad:** podrás gestionar tu cuenta de pago y efectuar operaciones no solo a través de la banca electrónica de tu banco, sino también a través de Agregadores Financieros (aplicaciones que recogen información de varias entidades bancarias). Tu banco también puede darte la posibilidad de agregar dentro de su banca electrónica la información del resto de entidades donde tengas cuentas.
- **Más agilidad:** las reclamaciones que interpongas ante la entidad y sean respecto a Servicios de Pago serán contestadas en 15 días hábiles.
- **Más movilidad:** los consumidores tienen un derecho de traslado de cuentas de pago de un proveedor a otro de manera gratuita y mediante la cumplimentación de un formulario. Este traslado incluirá toda la información necesaria para el traslado, las órdenes permanentes, transferencias y adeudos, las transferencias entrantes y emitidas a la cuenta de pago original, así como todos los fondos. Este traslado solo puede denegarse en casos tasados, como la existencia de obligaciones de pago exigibles y pendientes.

PSD2: Más seguridad en tus compras en comercio electrónico

Con la entrada en vigor de la nueva Directiva Europea de Servicios de Pago (PSD2) se incrementará la seguridad en las compras que efectúes en comercio electrónico.

¿Cómo aplicará este incremento de la seguridad en el momento de la compra?

Hasta ahora, cuando compras en internet en los comercios que utilizan un sistema de pago seguro, validamos tu identidad solicitándote en el momento del pago que introduzcas una clave de 6 dígitos que se envía a tu dispositivo móvil. En cambio, en los comercios que no utilizan este sistema de pago seguro puedes comprar sin esta clave.

Con la aplicación de la nueva normativa, antes de que finalice 2020 todos los comercios electrónicos que operan en Europa deberán utilizar el sistema de comercio electrónico seguro.

Esto quiere decir que **validaremos tu identidad en la mayoría de las compras en comercio electrónico** que realices desde tu ordenador o cualquier dispositivo móvil. La validación ya no se realizará introduciendo la clave de 6 dígitos, si no que deberás confirmar la compra a **través de la app CaixaBankNow desde un dispositivo móvil de confianza.**

¿Cómo hacer que tu dispositivo móvil sea de confianza?

La primera vez que accedas a la app CaixaBankNow desde un dispositivo móvil, te pediremos que valides tu identidad mediante un código que te enviaremos a tu teléfono o con la aplicación CaixaBank Sign si la tienes descargada.

¿Cuándo empezaré a validar mis compras con CaixaBankNow app?

Este cambio empezarás a notarlo a partir del verano 2020, por lo que es importante que tengas descargada la aplicación CaixaBankNow y las notificaciones activadas. [Acceso a descarga de la app CaixaBankNow](#)

Aunque será un proceso sencillo, pondremos a tu disposición tutoriales de cómo realizar el nuevo proceso de validación cuando hagas una compra.

Recomendaciones para reforzar la seguridad en tus medios de pago

- En caso de pérdida de tu dispositivo móvil, deberás llamar al servicio de Atención de CaixaBankNow 24h 93 887 25 25/900 40 40 90 o si estás en el extranjero el +34 938 87 25 25, y bloquearemos tu identificador de CaixaBankNow.
- Es importante que tengamos actualizado tu teléfono móvil y tu dirección de correo electrónico. Son los medios con los que nos comunicaremos contigo en caso de que detectemos cualquier incidencia que pueda afectar a tu seguridad. Puedes actualizar tus datos entrando en CaixabankNow, en Configuración (parte superior derecha) > Modificar mis datos personales > Modificar teléfonos o Modificar correo electrónico.
- Y recuerda, que si te detectas una operación sospechosa en alguna de tus tarjetas, tú mismo puedes limitar la operativa de tus tarjetas, como reintegros en cajeros o compras por internet y bloquear temporalmente tus tarjetas de forma fácil y rápida. [Consulta aquí más información](#) de cómo hacerlo.

Whatsapp: Un gran instrumento para los ciberdelincuentes

Whatsapp, es una de las aplicaciones de mensajería instantánea más usadas del mundo.

Este tipo de aplicaciones han permitido cambiar por completo la manera de comunicarnos. Lo que antes era una llamada telefónica o un mensaje de texto, ahora es un mensaje instantáneo gratuito en el que podemos incluir imágenes, videos, documentos, contactos, notas de voz o incluso, nuestra ubicación.

El éxito de esta aplicación y el uso intensivo que hacemos de ella hace que sea también **un instrumento ideal para que los ciberdelincuentes puedan contactar con sus potenciales víctimas.**

En los últimos meses, muchos son los usuarios de esta plataforma que están recibiendo, desde un **número desconocido**, mensajes en un tono afectuoso y familiar. Estos mensajes, pueden indicar, sin decir nombres ni datos, que es alguien que tiene un buen recuerdo nuestro o alguien que tiene ganas de vernos. **El objetivo es posteriormente sondarnos para que facilitemos nosotros la información de la persona de la que se podría tratar.**



Otra técnica de ingeniería social

Esto no es más que una técnica de **ingeniería social** empleada por ciberdelincuentes, con el objetivo de manipularnos y engañarnos para obtener información nuestra y de nuestro entorno para así, poder estafarnos.

¿Y cómo funciona?

Una vez **consiguen los datos** de una persona de nuestro entorno (que podría ser la que está contactando con nosotros), los ciberdelincuentes van a seguir el juego y van a hacernos creer que esta persona tiene problemas económicos y necesita dinero para solventar una **situación urgente**.

Es habitual en este tipo de estafa que el ciberdelincuente se haga pasar por nuestra hija o hijo y nos diga que se le ha estropeado el teléfono móvil y necesita dinero urgente para comprar uno nuevo.

Otro ejemplo recurrente es cuando el ciberdelincuente se hace pasar por un familiar que ha quedado retenido junto con sus maletas en el aeropuerto y necesita dinero para poder salir de él.

Los pretextos pueden ser muy variados:

Hay que tener presente que la intención del ciberdelincuente va a ser ganarse nuestra confianza, manipularnos y engañarnos para conseguir que le enviemos nuestro dinero o incluso, nuestros datos personales o bancarios.

¿Cómo podemos evitar ser víctimas de esta estafa?

En primer lugar, aplicar el sentido común y no ser confiado van a ser nuestras mejores armas.

- Siempre que recibas un mensaje instantáneo de alguien desconocido, extrema las precauciones.
- Antes que nada **pregunta el nombre de esta persona**.
- Haz **preguntas adicionales** que **te ayuden a verificar** que realmente esta persona que contacta contigo es quien realmente dice ser (por ejemplo, haciendo preguntas que sepas que sólo tú y esta persona sabéis la respuesta). Establecer una videollamada también puede ser útil para verificar su identidad.
- Estate alerta ante **expresiones** y **faltas de ortografía** que te puedan resultar sospechosas.
- **Si alguien te pide dinero, no se lo envíes** sin antes asegurarte bien de la identidad de esa persona. Lo más recomendable es que lo confirmes

usando los datos y medios habituales que tienes para contactar con esa persona.

Y, por último, nunca facilites tus datos bancarios ni personales a través de emails, mensajes, llamadas ni ningún otro canal.

No declares tus impuestos a los ciberdelincuentes

La campaña de la declaración de la renta, que empieza el 3 de Abril, no pasa desapercibida y da el espacio oportuno para que los ciberdelincuentes intenten llevar a cabo sus ataques para acceder a información personal y bancaria. Entre los principales peligros destacan los fraudes por correos de **phishing**, SMS de **smishing**, **llamadas fraudulentas**... Cualquiera de estas vías puede ser peligrosa. Para prevenir un posible fraude y **minimizar** los riesgos, es muy importante que extremes los cuidados y que sigas las sugerencias que propone CaixaBank para que puedas identificar si estás siendo víctima de un fraude.

¿Cómo sé si estoy siendo víctima de un fraude?

1. Revisa siempre el remitente desde donde te llega la información:

Muchas veces el dominio es parecido pero no el mismo. Esto nos puede llevar a confusión y, por no fijarnos, podemos caer en la estafa. Por ejemplo, el dominio oficial de la Agencia Tributaria es aeat.es. Los ciberdelincuentes pueden crear uno muy parecido, como por ejemplo aeatr.es. Ante la duda, asegúrate de cuál es la web oficial y tecléala directamente en el navegador sin utilizar enlaces de correos o SMS sospechosos.

2. Sospecha si te están solicitando información bancaria: La Agencia Tributaria o cualquier otra entidad nunca te va a solicitar información confidencial, económica o personal. Duda siempre de correos o SMS que te soliciten datos bancarios.

3. Comprueba el canal y el contenido del mensaje: La Agencia Tributaria solo utilizará el correo electrónico o SMS para informarte del estado de tu declaración o para avisarte si tuvieras una notificación en tu sede electrónica. Pregúntate si la Agencia Tributaria o cualquier otra entidad te solicitarían información confidencial, económica o personal por ese medio.

4. Fíjate en el tono del mensaje: Observa con detenimiento cómo está escrito el mensaje, ya que las faltas de ortografía son un signo claro de que el mensaje puede ser fraudulento. Aun así, cada vez abundan más los correos falsos correctamente redactados. También suelen intentar crear sensación de urgencia o de importancia para incentivarnos a caer en el fraude.

5. Revisa si hay archivos adjuntos o enlaces: Los mensajes fraudulentos suelen contener archivos adjuntos o enlaces como cebo de su estafa. [No abras](#)

nunca ningún enlace o documento sospechoso. La Agencia Tributaria nunca adjunta archivos con supuestas facturas u otro tipo de datos.

6. Si te contactan vía telefónica: Hay ciberdelincuentes que pueden usar técnicas de engaño avanzadas para ocultar su número real detrás de uno legítimo. Recuerda que ni la Agencia Tributaria ni ninguna otra entidad legítima te llamarán por teléfono solicitando tus datos personales o financieros ni tampoco te contactarán por este medio. Si necesitas comunicarte con ellos, puedes llamarlos a los teléfonos que indican en su página web oficial.

Y si detectas operaciones sospechosas en tu cuenta o has facilitado tus datos en lo que crees que es una campaña de fraude, contacta inmediatamente con tu gestor de oficina o llama al servicio de atención al cliente 24 h 93 887 25 25/900 40 40 90 o, si estás en el extranjero, el +34 938 87 25 25.

Manipulación de números de teléfono en llamadas entrantes ¿es posible?

La respuesta es sí y cada vez los ciberdelincuentes lo usan con mayor frecuencia.

Hay que tener en cuenta que el objetivo de los delincuentes digitales es conseguir **engañar a las víctimas para así poder sustraerles dinero, datos personales y datos bancarios sin que estas personas se den cuenta que están siendo víctimas de un fraude** (a esto se le denomina ingeniería social).

Suplantación de números de teléfono (Caller ID spoofing)

Uno de los medios que usan los ciberdelincuentes para estafar a sus víctimas es el teléfono. **Mediante llamadas telefónicas, el ciberdelinciente se hace pasar por un empleado del banco**, un técnico de una compañía informática, un operador de telefonía, una empresa de inversiones o cualquier otro tipo de empresa, **con el objetivo de conseguir, mediante diferentes pretextos, que la víctima haga un pago o bien, facilite sus datos bancarios y personales**.

Aunque haya personas que les puede extrañar una llamada telefónica de este tipo, **¿qué ocurre si el número de teléfono que aparece en la pantalla de su teléfono es un número legítimo?** Esta es una técnica que los ciberdelincuentes están usando con mayor frecuencia en los casos de fraude telefónico, y es lo que **se denomina suplantación de los números de teléfono en llamadas entrantes** (o en inglés, *Caller ID spoofing*).

Con esta técnica, **el ciberdelinciente consigue enmascarar su número de teléfono detrás del número de teléfono legítimo de la empresa** o institución por la que se está haciendo pasar. De esta manera, consigue: un mayor anonimato y una enorme capacidad de engaño.

SIM SWAPPING

El **SIM swapping** es un tipo de fraude que consiste en **obtener un duplicado de la tarjeta SIM de la víctima** para poder hacerse con el control de las comunicaciones de su teléfono móvil. Para ello, previamente el ciberdelincuente consigue **información personal y confidencial** de la víctima, habitualmente a través de técnicas de ingeniería social como pueden ser el Phishing, el Smishing o el Vishing, para poder **suplantar su identidad** y contactar telefónicamente con su compañía telefónica para que le facilite un duplicado de la tarjeta SIM. En ocasiones, es posible que incluso, se llegue a conseguir esta tarjeta SIM mediante la tramitación de una portabilidad de la línea a otra compañía telefónica.

Una vez el ciberdelincuente tiene en su poder la nueva tarjeta SIM y la activa, ya tiene **el control total** de las comunicaciones de esa línea telefónica: podrá recibir llamadas, emitirlas, leer o enviar mensajes de texto. Por el contrario, **la víctima, perderá el acceso telefónico** y por consiguiente, la cobertura, al desactivarse de forma automática su tarjeta SIM.

En este momento, el ciberdelincuente aprovechará para hacerse con el control de la **Banca Online de la víctima** usando los SMS de verificación que las entidades financieras suelen enviar a los teléfonos móviles de sus clientes.

¿Qué se debe hacer para evitar ser víctima de un fraude telefónico?

- **Aplicar sentido común y evitar prisas**

Ante cualquier llamada telefónica en la que soliciten datos personales y/o bancarios o realizar una operación (una transferencia por ejemplo), nunca facilitar ningún dato ni hacer ningún pago.

- **Tener en cuenta las técnicas de engaño avanzadas**

Hay que tener en cuenta que los ciberdelincuentes pueden usar técnicas avanzadas para ocultar su número de teléfono detrás de uno legítimo.

- **Contactar con la compañía telefónica en caso de pérdida de cobertura permanente**

Es recomendable contactar con la compañía para verificar el estado de la línea y de la tarjeta SIM.

Y si detectas operaciones sospechosas en tu cuenta o has facilitado tus datos en lo que crees que es una campaña de fraude, contacta inmediatamente con tu gestor de oficina o llama al servicio de atención al cliente 24h 93 887 25 25 / 900 40 40 90 o si estás en el extranjero el +34 938 87 25 25.

Esquiva las nuevas trampas de los ciberdelincuentes

Es en los momentos de cambio y transformación cuando los ciberdelincuentes saben que los usuarios son más vulnerables a sus ataques. Con el inicio de la pandemia mundial, por ejemplo, se aprovecharon del miedo causado por la urgencia sanitaria y utilizaron [el coronavirus como cebo para sus ciberataques](#).

En la actualidad, con la fusión de CaixaBank y Bankia, son los millones de clientes quienes deben estar más alerta que nunca ante posibles estafas dirigidas a ellos, ya que [los ataques que suplantan la identidad de CaixaBank y Bankia siguen creciendo](#).

Los mensajes que emplean los ciberdelincuentes van evolucionando, ya que los adaptan a la actualidad del proceso de fusión y al día a día de los clientes, siendo ahora mismo la transición de la antigua banca electrónica de Bankia a la app CaixaBank NOW el cebo principal de sus mensajes ilegítimos.

¿Cómo puedes identificar estos ataques?

Estas estafas pueden usar múltiples vías de ataque, incluso [combinar más de una a la vez](#) para tratar de ganarse la confianza de la víctima. Ya sea mediante correos electrónicos, SMS falsos o llamadas fraudulentas, generalmente los ciberdelincuentes tratan de **transmitir siempre una sensación de urgencia** a la víctima utilizando argumentos de máxima actualidad. Estos invitan a clicar en un enlace ilegítimo con el fin de que la víctima introduzca datos confidenciales en una web falsa o se descargue un malware. Una vez **el usuario teclea sus datos, estos pasan a estar en manos del ciberdelinciente**, que puede usarlos con el fin de suplantar su identidad para, por ejemplo, tratar de acceder a su banca online.



Además, el aspecto de estos ataques puede ser muy diverso: con algún error en el texto o escritos sin una sola falta ortográfica; con los logotipos de CaixaBank y Bankia inventados o con los oficiales, copiados de sitios legítimos. **Se debe desterrar la falsa creencia de que todos los mensajes ilegítimos están mal escritos o presentan un aspecto descuidado.** Los ciberdelincuentes siguen sofisticándose y creando mensajes cada vez más difíciles de distinguir.

¿Cómo puedes esquivarlos?

Los internautas deben aprender a analizar con atención todas las comunicaciones que reciben antes de abrir cualquier enlace o documento adjunto y de revelar información a terceros por cualquier vía siguiendo estos puntos clave:

La regla de oro para no caer en este tipo de estafas

Accede a CaixaBank Now exclusivamente desde la app oficial o vía www.caixabank.es.

Recuerda que ni CaixaBank ni ninguna otra empresa o institución legítima pide a sus clientes que revelen las claves de acceso de su banca digital o servicio online. Nunca se deben compartir las contraseñas con nadie, ni otros datos personales ni el teléfono móvil.

Si es urgente, no corras: sospecha

Generalmente los ciberataques que reciben los usuarios informan por SMS o correo falso (smishing y phishing respectivamente) de que sus cuentas bancarias han sido bloqueadas. Es un asunto que puede provocar preocupación en el usuario

y que puede provocar que clique y revele información (usuario y contraseña) sin reflexionar en la **coherencia y procedencia del mensaje**.

Por eso, antes de realizar ninguna acción, piensa: **¿Tiene sentido que mi banco, esta persona o cualquier otra empresa me mande este mensaje?**

¿El remitente es quién dice ser?

El cuerpo del mensaje, el asunto, la firma, los logos... todos estos elementos se pueden manipular fácilmente en un correo de **phishing**, tratando de suplantar la identidad de cualquier persona o institución como CaixaBank. Incluso el remitente, la dirección desde la cual se manda el correo, puede manipularse y mostrar una dirección muy similar o incluso igual que una dirección legítima de la entidad.

Del mismo modo ocurre con los **SMS falsos**. Tanto el texto del mensaje como el número de teléfono que aparece en la pantalla, se pueden llegar a manipular y mostrar uno muy parecido o igual que el teléfono legítimo.

Por eso, lo **primero es analizar con detalle** la dirección de correo o el número de teléfono del remitente para descartar **posibles manipulaciones**.

Mira por donde clicas

Para asegurar que los enlaces de los mensajes son legítimos, es necesario **comprobar a dónde conducen antes de abrirlos**. Pero si están en un SMS, la opción más segura es **acceder a la información que se ofrece a través de la app oficial o de la página web del servicio**.

Sal de dudas

Si aun así no puedes asegurar al 100% la legitimidad del mensaje ya provenga de un amigo, un compañero de trabajo o una empresa, **antes de clicar en enlaces o anexos**, siempre es aconsejable **contactar con el remitente por otro canal oficial** (telefónicamente, por ejemplo). De esta forma podremos confirmar si el mensaje recibido es o no legítimo.

SMS y llamadas fraudulentas:

La nueva combinación que los ciberdelincuentes usan para robar datos bancarios

Correos de **phishing**, SMS de **smishing**, webs falsas, **llamadas fraudulentas**, dispositivos externos USB infectados... Por separado, cualquiera de estas vías de ataque puede ser muy peligrosa, **¿pero qué pasa si se utiliza más de una en la misma estafa?**

Existe un **nuevo tipo de fraude que combina los SMS falsos y las llamadas fraudulentas** para robar datos bancarios y acceder a la banca online de la víctima.

¿Por qué unir dos vías de ataque en una misma estafa?

En el fraudulento arte de la suplantación de la identidad, **lo más importante es ser lo más persuasivo posible**. Los cibercriminales saben que cuanto más

complejo sea el ataque, más realista parecerá a ojos de la víctima y más fácil será que esta caiga en la trampa.

¿Cómo funcionan este tipo de estafas?

En la primera fase, **el usuario recibe un SMS** firmado supuestamente por CaixaBank animándolo a clicar en un enlace. Para que sea menos sospechoso, **los ciberdelincuentes son capaces de engañar a tu dispositivo** para que sitúe su mensaje falso a continuación de los mensajes legítimos que hayas recibido previamente de CaixaBank, en el mismo hilo de SMS.

Al clicar, aparece una web falsa, que imita a la de CaixaBank, solicitando la introducción de datos personales como el usuario, la contraseña y el teléfono.

El Fraude del Romance:

Cuando las redes sociales de citas se convierten en una oportunidad para los ciberdelincuentes

Miles de personas recurren a **aplicaciones de citas o páginas web de contactos** para conocer a gente y quien sabe, encontrar una relación amorosa. Esta práctica, **cada vez más extendida**, supone una ventaja para los usuarios al permitir contactar con múltiples personas de forma rápida, sencilla y desde cualquier lugar. No obstante, **esta práctica no pasa desapercibida por los ciberdelincuentes** que aprovechan estas plataformas y el **exceso de confianza** que predomina entre sus usuarios, para buscar **potenciales víctimas a las que estafar**.

¿Cómo funciona este fraude?

El Fraude del Romance es un tipo de fraude cuyo objetivo es **atacar a los sentimientos y la confianza de la víctima** como principal baza para convencerla y así lograr **engañarla** para conseguir estafarle **grandes cantidades de dinero**.

El *modus operandi* es el siguiente:

- **El ciberdelincuente crea perfiles falsos** en aplicaciones de citas y páginas web de contactos con fotografías y descripciones que **llaman la atención al usuario**.
- Se establece **el interés y se inicia la conversación** entre el ciberdelincuente y la víctima.
- Durante días, semanas e incluso meses, el ciberdelincuente **va ganándose la confianza** de la potencial víctima y la va **seduciendo**. Suele mostrarse como una persona con una **profesión que llama la atención**, como es la de ser un **soldado americano**, el **trabajador de una planta petrolífera**, un **capitán de barco**, un **médico humanitario**, entre otros.

- **Se inicia una relación a distancia.** Lo más habitual es que esta relación se inicie sin verse en persona pero que **exista la promesa de conocerse** próximamente.
- Para poder viajar para conocerse o bien porque le ha surgido un problema muy grave, el ciberdelincuente **pide a la víctima que le envíe dinero**. La víctima al estar **totalmente engañada** procede a hacer el envío del dinero solicitado. En ocasiones, **el dinero solicitado obliga incluso a que la víctima se endeude** con su entidad financiera.
- Una vez el ciberdelincuente recibe el dinero que ha estimado oportuno o ve que no puede continuar con el engaño, **procede a cortar toda comunicación con la víctima**.

¿Qué recomendaciones de seguridad se han de seguir para evitar ser víctimas de este tipo de fraude?

Desde CaixaBank se quiere trasladar algunas recomendaciones de seguridad para minimizar los riesgos de ser víctima del fraude del romance:

- **No ser confiado, aplicar el sentido común y no tener prisa.**
- **Revisar los perfiles** de las redes sociales de citas o páginas de contactos. **Prestar atención y desconfiar** de los perfiles recientemente creados y/o los que tengan fotografías que parezcan de anuncio.
- **Desconfiar ante las prisas, urgencias o pretextos extraños en la que se solicite el envío de dinero.**
- **No facilitar información confidencial** con terceros.

¿Cómo se debe actuar en caso de ser víctima de fraude?

En caso de ser víctima de este tipo de fraude, se debe:

- Poner el fraude en conocimiento de la entidad bancaria de la que se sea cliente con la mayor celeridad posible.
- Interponer una denuncia policial.
- Guardar todos los datos e información relativa al anuncio y a los contactos establecidos con el supuesto vendedor, ya que pueden ser requeridos durante la investigación del caso.
- Denunciar el perfil en la aplicación o página web para que se proceda a la baja de dicho usuario.

Si el usuario envía los datos solicitados, **recibe una llamada del ciberdelincuente haciéndose pasar por un gestor de CaixaBank**. Para hacerlo todavía más complicado, el número falso que aparece en pantalla es muy similar o incluso igual que uno legítimo de la entidad.

Si quieras conocer todos los detalles de este ataque, [en el blog de CaixaBank encontrarás una explicación más detallada](#).

¿Cómo protegerse de este fraude?

- Recuerda que ni CaixaBank ni ningún otro servicio legítimo **te pedirá nunca tus datos personales, teléfono o claves secretas de acceso**. [No las compartas con nadie](#).
- **Te recomendamos no clicar directamente en los enlaces de los SMS.** Es mejor acceder a la información que se ofrece a través de la propia app o de la página web del servicio. En CaixaBank, puedes [activar las notificaciones en tu móvil](#) a través de la App para recibir la información de una forma más fiable y segura.
- Aunque este fraude es más elaborado debido a que combina dos vías de ataque para parecer más legítimo, si recuerdas que CaixaBank nunca te pedirá que introduzcas datos personales, claves ni teléfono, sabrás fácilmente que se trata de un fraude. Por lo tanto, **prestar mucha atención y el sentido común** son y serán siempre tus mejores aliados.

Suplantación de identidad (fraude CEO + fraude facturas)

La suplantación de identidad en internet se produce cuando una persona se hace pasar por otra con el fin de cometer un acto ilegal o un perjuicio. En el mundo empresarial es habitual que se haga con el fin de obtener dinero o información confidencial, aunque los motivos pueden ser varios.

Nadie está a salvo de este delito ni puede tener la certeza de que nunca le ocurrirá. Todos somos susceptibles de convertirnos en víctimas de este tipo de fraude, que puede acarrear graves daños económicos y de imagen.

Conocer los distintos tipos de estafa, saber cómo se producen y cómo actuar en caso de que sucedan son los primeros pasos para prevenir la suplantación de identidad en las empresas.

Fraude al CEO

¿Qué es?

El fraude al CEO es una estafa basada en la [ingeniería social](#) dirigida a empresas. Los ciberdelincuentes suplan un alto cargo de la compañía con el propósito de

engaños a los empleados para que, en la mayoría de los casos, efectúen órdenes de pago fraudulentas.

¿Cómo funciona?

El estafador estudia las víctimas y recaba información sobre la empresa. Una vez conoce el organigrama y las operaciones habituales de la compañía, suplanta la identidad del CEO o de un alto cargo de la organización, generalmente a través del *hackeo* de su cuenta correo o de la creación de una dirección falsa. Luego, inicia el envío de correos electrónicos o rondas de llamadas para solicitar el pago a un tercero, siempre de forma urgente y confidencial. El objetivo es desalentar a la víctima de verificar la operación.

Una vez recibidas las instrucciones, el empleado engañado lleva a cabo los pagos solicitados a las cuentas que controla el estafador.

¿Qué puedes hacer para prevenir el fraude al CEO en las empresas?

- Ante cualquier petición sospechosa, confirma la legitimidad de la operación por otra vía de comunicación. Ya sea vía telefónica o por correo electrónico, es importante establecer un sistema de doble verificación con el directivo responsable. Los estafadores querrán mantener el asunto bajo la máxima confidencialidad para que no hagas las debidas comprobaciones.
- Aunque provengan de altos cargos de la empresa, no te sientas presionado si recibes solicitudes urgentes. Sigue los procedimientos habituales. Recuerda que transmitir prisa al trabajador es una táctica común entre los estafadores.
- Sé precavido con la información que difundes en las redes sociales sobre la empresa y el cargo que ostentas. Los atacantes utilizarán toda la información que esté a su alcance para perpetrar la suplantación de identidad.
- Si finalmente se ha llegado a ejecutar la operación fraudulenta, debes informar urgentemente a la sucursal bancaria e interponer una denuncia a la policía. La rapidez es un factor clave para frenar la estafa y minimizar los posibles daños.
- No debes borrar los correos electrónicos, registros telefónicos o documentación que hayan aportado los estafadores. Son pruebas y pueden ser necesarias para una investigación policial.

Fraude de facturas

¿Qué es?

El fraude de facturas es una estafa basada en la [ingeniería social](#) dirigida a empresas. Se produce cuando el estafador suplanta la identidad de un proveedor o de un empleado con el fin de desviar el cobro de facturas.

¿Cómo funciona?

Los estafadores de facturas estudian las empresas a través de su página corporativa, redes sociales e incluso *hackeando* las cuentas de correo de los empleados. El objetivo es descubrir las relaciones que mantienen con sus proveedores, incluidos los detalles de los pagos regulares.

El ciberdelincuente suplanta el proveedor y se pone en contacto con la empresa para solicitarle un nuevo procedimiento de pago facilitando un nuevo número de cuenta bancaria fraudulenta.

A partir de este momento, la víctima enviará todos los pagos a la cuenta bancaria que controla el estafador. El fraude solo se puede descubrir cuando el proveedor legítimo reclama el impago de las facturas.

¿Qué puedes hacer para prevenir el fraude de facturas en las empresas?

- Cuando recibas una petición de cambio de número de cuenta bancaria por parte de un proveedor o acreedor, ponte en contacto con este por medio de una vía de comunicación distinta para confirmar la operación. Un sistema de doble verificación, sea vía telefónica o por correo electrónico, es indispensable para asegurar la legitimidad de la operación.
- Mira cuidadosamente cada factura y compárala con las facturas anteriores que sabes que son genuinas. Los detalles de la cuenta bancaria, la redacción utilizada y el logotipo de la compañía pueden darte pistas sobre la veracidad del documento.
- Considera la posibilidad de eliminar la información sobre clientes o proveedores de la página web de la empresa y de redes sociales. Dar a conocer tus relaciones laborales puede ser beneficioso para tu negocio, pero también se lo pondrá más fácil a los suplantadores de identidad.
- Si has sido víctima de la estafa y has efectuado transacciones al número de cuenta fraudulento, debes informar urgentemente a tu sucursal bancaria e interponer una denuncia a la policía. La rapidez con la que reacciones determinará el alcance de los daños.
- Nunca borres los correos electrónicos, registros telefónicos o documentación que hayan aportado los ciberdelincuentes. Son pruebas y pueden ser necesarias para una investigación policial.

Cualquier empresa puede de ser víctima de este y otros fraudes. Por este motivo, la formación y la concienciación en ciberseguridad es determinante para que los usuarios sean capaces de reconocer el fraude y denunciarlo a tiempo.

¿Qué es el malware RAT y por qué es tan peligroso?

Aunque este nombre se utilice también para referirse a un tipo de malware, originalmente el **RAT (Remote Administration Tool)** se creó con un buen

propósito: ayudar en remoto a gestionar configuraciones y solucionar problemas informáticos de forma instantánea y eficaz.

Por ejemplo, cuando autorizas a un técnico informático a tomar el control de tu equipo y este empieza a mover el cursor de tu pantalla, es gracias a un RAT legítimo, instalado previamente por el propio usuario para autorizar la conexión remota de alguien en quien confía.

Pero como cualquier otra aplicación digital, también puede ser utilizada para hacer el mal. **Al lado oscuro del RAT se le conoce con el nombre de Remote Access Trojan: un troyano informático que se cuela por la puerta deatrás de tu equipo.** En manos de los ciberdelincuentes, puede convertirse en un arma muy dañina.

¿Cómo actúa?

Generalmente la infección del malware RAT se realiza a través de algún método de **ingeniería social**. Los atacantes utilizan **técnicas de engaño** con el objetivo de que el usuario clique donde no debe y descargue el archivo malicioso en su dispositivo.

Generalmente los hackers pueden adjuntar un RAT en un correo electrónico en forma de archivo anexo o enlace o en una aplicación móvil, pero pueden utilizar muchos otros trucos para distribuir su malware. Entre otros, pueden esconderlo detrás de los anuncios emergentes que aparecen al navegar por distintas páginas web o incluso en servicios de entretenimiento online.

Por ejemplo, durante el confinamiento producido por la pandemia mundial del **COVID-19**, el consumo de cine tanto en streaming como por descarga directa o de Torrents se ha disparado. Los criminales no desaprovechan este canal y están consiguiendo infectar a usuarios **escondiendo su malware RAT en servicios de descarga o streaming de películas pirata**.

Además, continuamente adaptan la temática de sus estafas a la actualidad para resultar más atractivos. Argumentos como la declaración de la renta, preguntas relacionadas con el Coronavirus o el trabajo remoto, la liga de fútbol, las rebajas, el Black Friday, etc. Por lo tanto se debe poner especial atención ante comunicaciones de este tipo.

Sea como sea el método o el tema utilizado por el pirata informático, cuando la víctima cae en la trampa e instala el RAT en su equipo, sin saberlo le está concediendo acceso remoto a su dispositivo.

¿Qué puede hacer el RAT si consigue infectarme?

Si consigue infectar a su víctima y asumir el control remoto del equipo, **las posibilidades para el ciberdelincuente son infinitas**. Una vez dentro, el hacker puede tratar de **acceder a la aplicación de banca online de la víctima** para realizar transferencias, descubrir claves de acceso, suscribirse a servicios no deseados, furgonear en el buzón de correo electrónico, entrar en perfiles de redes sociales e incluso realizar copias de toda la galería de fotos, entre

otras **acciones que pueden ser devastadoras, tanto a nivel personal como corporativo.**

¿Cómo puedo evitar ser víctima de un RAT?

Para reducir los riesgos de infección, es imprescindible seguir unas **buenas prácticas digitales** a la hora de navegar por internet y tener mucho cuidado con descargar aplicaciones de origen desconocido.

Tampoco se debe clicar en enlaces o anexos de correos electrónicos sospechosos, aún si el remitente es aparentemente conocido. Actualmente circulan **campañas de phishing muy sofisticadas capaces de suplantar la identidad de bancos** o de cualquier otro servicio legítimo de forma muy realista y convincente. Por ello, al recibir un correo, se deben **analizar con detenimiento las señales** que ayudarán a determinar su veracidad.

Además de aplicar siempre el sentido común, otra de las medidas a seguir para reducir el riesgo de infección es **mantener siempre el sistema operativo del dispositivo actualizado** con la última versión disponible, al igual que las distintas aplicaciones que se utilicen y el antivirus. Éste debe estar configurado adecuadamente para que se actualice automáticamente y trabaje analizando constantemente los archivos en busca de posibles amenazas.

Creo que estoy infectado. ¿y ahora qué?

Aplicando todas estas medidas reduciremos drásticamente las posibilidades de ser infectados. Aunque por encima de todo, la mejor medida para combatir al RAT y a cualquier otro malware, es el sentido común, mantener siempre la alerta activa y revisar dos veces antes de clicar.

En el caso de saber o sospechar de una infección, lo más recomendable es formatear y reinstalar totalmente el dispositivo, dado que **los antivirus tampoco son garantía de detectar cualquier malware.**

Además, es probable que el RAT también haya tenido acceso a las contraseñas de cualquier otro servicio al que el usuario haya accedido con su dispositivo: redes sociales, tiendas online, servicios de streaming, etc. Por este motivo, una vez formateado el dispositivo, es también igualmente importante modificar las contraseñas de todos los servicios que se utilicen habitualmente, especialmente la del correo electrónico.

Si un cliente CaixaBank ha sido víctima de un fraude, recomendamos contactar con una de las dos opciones siguientes:

- Atención al cliente (Teléfono 24h): +34 938 87 25 25 / +34 900 40 40 90
- Su gestor de la oficina.

Veamos un ejemplo práctico: ataque real de RAT a clientes de entidades bancarias.

El RAT ataca a los clientes de diversas entidades financieras para obtener el control remoto de sus dispositivos.

En la mayoría de casos analizados, el malware se extiende a través de un correo electrónico malicioso utilizando por ejemplo el argumento de una supuesta factura.

Cuando el usuario abre el enlace o el documento adjunto del correo, puede instalar el RAT en el equipo, **cediendo sin darse cuenta el control remoto al ciberdelincuente**.

Sea cual sea el método que haya empleado el criminal para instalar el RAT en el dispositivo del cliente, **en el caso de clientes de CaixaBank** podría actuar de la siguiente forma:

Cuando el usuario abre la app CaixaBank NOW, el RAT le mostraría una pantalla de “**instalación del módulo de seguridad**”.



Es sólo una distracción. Mientras el cliente ve esta pantalla, el hacker está detrás operando con la app para realizar una transferencia.

Al hacerlo, el cliente recibe una alerta en su móvil para autorizar la transferencia fraudulenta. **Si el cliente no se fija correctamente en los datos relacionados con la autorización**, aceptará la operación desconocida en favor del hacker.

Por eso antes de introducir un código recibido por SMS o firmar una operación a través de la app CaixaBank Sign o de cualquier otra aplicación móvil bancaria, **antes de autorizar nada, es importantísimo examinar detenidamente los datos de la operación (importe, cuenta destino)**, incluidos en los SMS y en las solicitudes de firma de las app móviles.

En resumen...

Las principales recomendaciones son:

- Atención máxima a la hora de autorizar cualquier operación y revisar los datos asociados: cuenta destino e importe.
- Mantener los dispositivos, aplicaciones y antivirus actualizados.
- Reportar cualquier comportamiento sospechoso.
- Y sobre todo, aplicar siempre el sentido común y no precipitarse.

La compraventa online

Una oportunidad para los estafadores

El uso creciente de las tecnologías aplicadas a la compraventa de productos presenta muchas ventajas para los usuarios, pero también comporta una serie de riesgos a los cuales tienes que hacer frente.

Uno de estos riesgos es que, ya seas vendedor o comprador, puedes ser víctima de una estafa. Como usuario de estos servicios digitales de compraventa, te expones a realizar el pago de un producto que quizás nunca te llegará o bien, a enviar tu producto y no recibir nunca el pago acordado.

Portales como milanuncios, eBay o aplicaciones como Wallapop, son una manera muy rápida y sencilla de comprar o vender productos de forma online. No obstante, el uso masivo de estas plataformas hace que también los estafadores lo vean como una oportunidad para poder buscar potenciales víctimas.

¿Qué puedes hacer para evitar ser víctima?

- **No dar credibilidad a ofertas muy agresivas:** Siempre se tiene que desconfiar de productos con precios muy rebajados puesto que son el anzuelo perfecto para engañarnos. Se recomienda, antes de hacer la compra, estudiar cuales son los precios de mercado.
- **Analizar el perfil del usuario vendedor/comprador:** Habitualmente los estafadores no suelen facilitar muchos datos en sus perfiles y no disponen de fotografías reales, datos de contacto verificados, etc. Otro elemento que debe hacerte sospechar es cuando la fecha de creación del perfil es muy reciente.

Es importante también observar el comportamiento del vendedor/comprador, puesto que los estafadores acostumbran a insistir en el cierre de la transacción con celeridad o bien, en ocasiones, pueden pedir datos personales o bancarios que pueden usar para fines ilícitos.

- **Revisar comentarios:** Es importante dar un vistazo a lo que dicen los comentarios de los vendedores/compradores. Si no tienen ningún

comentario o los comentarios son negativos, se recomienda extremar precauciones.

- **Revisar bien el anuncio:** Los estafadores suelen usar imágenes falsas o manipuladas para poder engañar a las víctimas. En caso de duda, es recomendable pedir al vendedor imágenes adicionales o con algún distintivo (logotipos, u otros elementos de seguridad) que garanticen la veracidad del artículo.
- **Usar sistemas de pago seguros:** Se recomienda usar sistemas de pago que den más garantías, como los pagos vía Paypal, contra reembolso o los que ponen a disposición de los usuarios las mismas aplicaciones, como Wallapop.
- **Uso de excusas o pretextos:** Si se indica que es mejor continuar con la comunicación por algún canal más privado o hacer pagos por avanzado, puede ser un motivo claro para desconfiar y/o abstenerse de hacer el pago.
- **Denunciar el anuncio:** En caso de sospechar que un anuncio es falso, se recomienda denunciarlo a la plataforma que lo aloja para que pueda ser revisado y en todo caso, eliminado. Cualquier otra persona podría ser víctima del fraude.

La compraventa por Internet es un medio fácil y rápido para poder comprar y vender productos a otras personas. No obstante, no tienes que olvidar que también son una oportunidad rápida y fácil para que los estafadores te puedan engañar.

Por lo tanto, siguiendo estas recomendaciones, revisando bien lo que quieras comprar, no tener prisa y sobre todo, aplicando el sentido común, te ayudará a minimizar el riesgo de ser engañado a la hora de comprar o vender un artículo por Internet.

Seguridad en las tarjetas bancarias

Protege tus compras para disfrutar de la máxima tranquilidad

Un paso más allá en la seguridad de tus operaciones

Desde Caixabank, queremos que te sientas siempre seguro. Por eso, como cliente de CaixaBank podrás solicitar la devolución de compras y operaciones que no reconozcas durante los 13 meses posteriores a la fecha de operación para que estudiemos tu caso.

Además, tienes a tu disposición el teléfono exclusivo para clientes **93 887 25 25** o **900 40 40 90** a través del que:

- Te ayudaremos a resolver tus dudas y consultas siempre que lo necesites.
- Podrás comunicar si sospechas que has sido víctima de un fraude o si has identificado una operación que no reconoces.

También, te mantendremos al día de los fraudes más frecuentes y te damos las claves de cómo evitar ser víctima de éstos a través de tu correo electrónico. Si no lo

recibes, ponte en contacto con tu oficina para comprobar que disponemos de tu dirección de correo electrónico actualizada.

Control de uso

Esta opción te permite activar o desactivar temporalmente y para cada una de tus tarjetas, operativas determinadas como las compras en internet, en el extranjero, en ocio para mayores de 18 años, en aerolíneas, en hoteles... o la retirada de efectivo en cajeros.

Consulta [aquí](#) más información.

Bloqueo de tarjeta

Con esta opción puedes “apagar” de forma temporal o permanente tu tarjeta. Te recomendamos el bloqueo temporal si no sabes dónde tienes tu tarjeta o si no la vas a usar durante un tiempo. El bloqueo permanente es la mejor opción si has perdido o te han robado la tarjeta¹.

Consulta [aquí](#) más información.

CaixaBankProtect

Es un servicio unido a la tarjeta que consiste en enviar alertas sobre las operaciones realizadas con la tarjeta. Esas alertas se envían a través de mensajería SMS o de push en la app de CaixaBankNow o mediante correo electrónico. Las alertas informan, por ejemplo, sobre:

- operaciones con un importe que supera los 500 €,
- reintegros (retiradas de dinero) en el cajero superiores a 1.000 €, y
- primeras compras realizadas en el extranjero, cualquiera que sea su importe.

CaixaBankProtect Emergency

Este servicio permite que, si pierdes o te sustraen la tarjeta en el extranjero, puedas solicitar el envío de una tarjeta de sustitución o bien solicitar retirar dinero en efectivo, a través de una empresa corresponsal de CaixaBank en la gran mayoría de países.

- Envío de una tarjeta urgente de sustitución: El precio de este servicio, se informará en el momento de solicitar la tarjeta ya que puede variar en función del país en el que te encuentres y de la urgencia del envío.
- Retirada de efectivo: La cantidad de dinero que te enviaremos no podrá superar el límite de crédito disponible de tu tarjeta. Si fuera necesario convertir tu dinero a una divisa distinta al euro, el corresponsal podrá aplicarle la comisión que corresponda por el cambio de divisa.

¿Tienes dudas sobre nuestra banca digital?

[¿Cómo puedo recuperar las claves de acceso a CaixaBankNow?](#)

Puedes restaurar tus claves de acceso a CaixaBankNow online haciendo clic en el siguiente [enlace](#). Para ello necesitas tener a mano una tarjeta de crédito o débito de CaixaBank y el teléfono móvil que tienes en tus datos de contacto en Configuración personal. En caso contrario, solo podrás restaurar tus claves de acceso en tu oficina de CaixaBank.

[¿Cómo puedo darme de alta en CaixaBankNow si ya soy cliente de CaixaBank?](#)

Date de alta siguiendo [este enlace](#) o descárgate la App CaixaBankNow para hacerlo de manera más fácil desde tu móvil. Solo necesitarás introducir tus datos personales, tu teléfono móvil y nos encargaremos de validar contigo esta información. Te proporcionaremos tus claves de acceso y al instante, podrás acceder a tu banca digital desde cualquier dispositivo. ¡Así de fácil!

Accede a más información [aquí](#).

[¿Cómo consultar mi información fiscal?](#)

Puedes consultar tus comunicados fiscales dentro de CaixaBankNow, en tu MailBox, en el apartado "Correspondencia".

[¿Cómo activo la firma dentro de la app CaixaBankNow?](#)

1. Abre la app CaixaBankNow e inicia sesión con tus claves.
2. Ve a tu "Perfil".
3. Selecciona "Seguridad" y elige "Firma".
4. Sigue las indicaciones para activar la firma en tu dispositivo.

[¿Cómo puedo concertar una cita con mi gestor?](#)

Puedes solicitar cita previa accediendo a 'Mi oficina' o 'Mi gestor', en la parte superior derecha de la pantalla de CaixaBankNow. Además, también puedes gestionar las citas solicitadas. Si no te aparece esta opción de menú, es porque no tienes asignado ningún gestor personal.

Accede a más información [aquí](#).

[¿Cómo puedo descargar los movimientos de mis cuentas y tarjetas?](#)

Puedes descargar un fichero desde el apartado "Descargar ficheros" a través de tu cuenta CaixaBankNow. Ten en cuenta que una vez realizada la primera descarga, o

si ha pasado 1 mes desde la recepción del fichero, el fichero pasará a la lista "Histórico de ficheros recibidos" por un periodo máximo de 3 meses.

Accede a más información [aquí](#).

¿Qué es una solicitud de pago?

Es una notificación por la que un emisor solicita un pago a un cliente

¿Sigue siendo necesaria la app CaixaBank Sign para firmar las operaciones de la banca digital?

No, una vez que actives la firma en CaixaBankNow, ya no necesitarás la app CaixaBank Sign y podrás eliminarla de tu dispositivo. Si tienes más de un identificador, recuerda activar la firma en cada de tus identificadores antes de eliminar la app.

Noa, el asistente virtual de CaixaBankNow

¿Tienes dudas con la contratación de un producto o, quieres hacer una consulta sobre CaixaBank o sobre CaixaBankNow? Pídele ayuda a Noa.

Basado en una avanzada inteligencia artificial, ahora tiene una **mayor capacidad de respuesta** para entender y contestar tus preguntas de forma fluida y natural, tanto por escrito como por voz.

Resuelve cualquier duda sobre productos y servicios CaixaBank.

Es más inteligente y cuenta con nuevas consultas personalizadas.

Más de 1,8 millones de clientes ya hablan con Noa habitualmente.

Pregúntale lo que necesites a través de **la web y la app de CaixaBankNow**

¿Desde dónde quieres consultar a Noa?

Web

Entra en la web con tus datos de usuario de CaixaBankNow.

Accede a Noa a través de la web de CaixaBankNow. Encontrarás el asistente tanto en la parte superior derecha, en el ícono de Noa, como en el botón flotante de la parte inferior derecha.

Haz una consulta sobre algún producto o servicio de CaixaBank. Por ejemplo, escribe: “Quiero contratar una tarjeta” o “Quiero hacer una transferencia”.

Noa resolverá tu duda y, a continuación, podrás hacer una nueva consulta o continuar utilizando otras funciones de la web.

¿Desde dónde quieres consultar a Noa?

App

Si no tienes instalada la app de CaixaBankNow en tu móvil, descárgatela desde Play Store o Apple Store.

Entra en la app con tus datos de usuario de CaixaBankNow.

Accede a la pantalla de Noa en la app de CaixaBankNow.

Haz una consulta sobre algún producto o servicio de CaixaBank. Por ejemplo, escribe o di: “¿Cómo puedo consultar el saldo de mi cuenta?”.

Noa resolverá tu duda y, a continuación, podrás hacer una nueva consulta o continuar utilizando otras funciones de la app.

Preguntas frecuentes sobre tu gestor CaixaBank

¿Cómo puedo acceder a la conversación con mi gestor?

Puedes acceder a la conversación con tu gestor a través del enlace 'Gestor'. Si no puedes acceder, es posible que no tengas un gestor asignado.

¿Cómo puedo eliminar una conversación con mi gestor?

Las conversaciones con tu gestor no se pueden eliminar.

[¿Cómo puedo pedir una cita con mi gestor?](#)

Puedes solicitar una cita desde la sección 'Gestor', nueva Cita Previa. Desde ahí también puedes gestionar las citas solicitadas. Si no te aparecen los datos de tu gestor, es posible que no tengas un gestor asignado.

[¿Cómo puedo acceder a una videollamada con mi gestor?](#)

Puedes acceder a la videollamada con tu gestor desde la sección 'Gestor', dentro de 'Cita Previa'. Si no te aparecen los datos de tu gestor, es posible que no tengas un gestor asignado.

[¿Cómo puedo enviar documentación a mi gestor?](#)

Para enviar documentación a tu gestor debes acceder a la sección 'Gestor', iniciar una conversación en el chat y pulsar el botón (+), situado junto al campo de texto, para adjuntar los documentos y enviarlos. Si no te aparecen los datos de tu gestor, es posible que no tengas un gestor asignado.

[¿Cómo puedo modificar o cancelar una cita?](#)

Para anular una cita, accede a la sección 'Gestor' y busca tu cita para cancelarla. Para modificar la cita, tienes que anular la existente y pedir otra. Si no te aparecen los datos de tu gestor, es posible que no tengas un gestor asignado.

[¿Cómo puedo solicitar una cita por videollamada a mi gestor?](#)

Puedes solicitar una videollamada con tu gestor desde la sección 'Gestor'. Crea una nueva cita previa y selecciona 'Videollamada'. Si no te aparecen los datos de tu gestor, es posible que no tengas un gestor asignado.

[¿Cómo puedo contactar con mi gestor?](#)

Puedes contactar con tu gestor a través del enlace 'Gestor', donde encontrarás sus datos de contacto y un chat para escribirle directamente. Si no te aparecen los datos de tu gestor, es posible que no tengas un gestor asignado.

[Consulta de citas](#)

Puedes consultar tu historial de citas solicitadas desde la sección 'Gestor'. Si no te aparecen los datos de tu gestor, es posible que no tengas un gestor asignado.