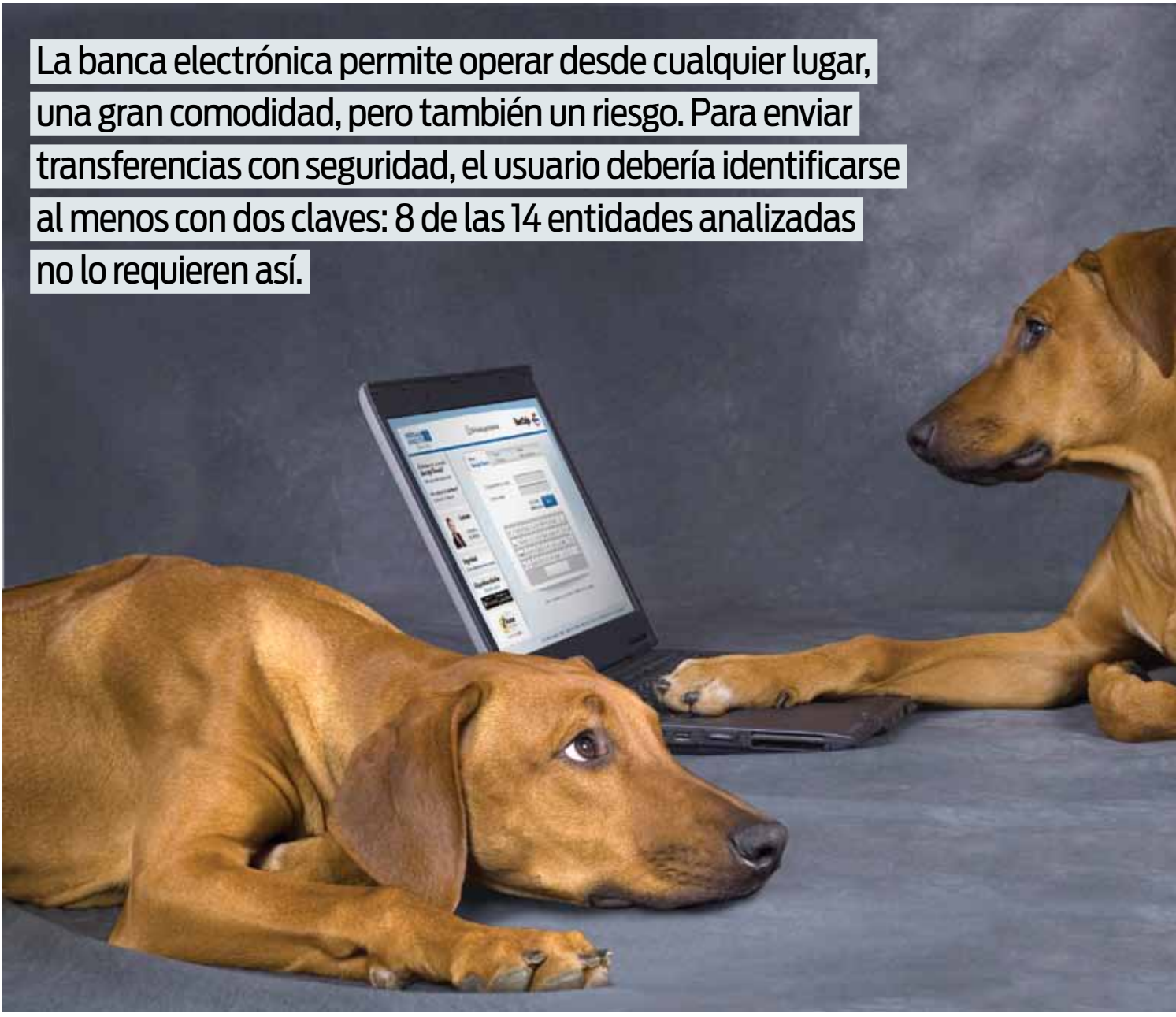
Mejor con doble clave

No hay método más seguro para realizar una operación bancaria que acudir en persona a la sucursal, dar la orden y guardar el comprobante escrito por si luego surge algún problema. Pero además de este sistema tradicional, las entidades bancarias nos ofrecen la posibilidad de realizar operaciones cómodamente desde cualquier ordenador, las 24 horas del día, gracias a las nuevas tecnologías e Internet. El uso de la banca electrónica se fomenta no solo por el beneficio que supone para los usuarios, sino también porque las entidades reducen costes en oficinas y personal, aunque sea a costa de un mayor riesgo

La banca electrónica permite operar desde cualquier lugar, una gran comodidad, pero también un riesgo. Para enviar transferencias con seguridad, el usuario debería identificarse al menos con dos claves: 8 de las 14 entidades analizadas no lo requieren así.



en las transacciones, que se minimiza con los protocolos de seguridad activados.

La información confidencial que circula por la red puede ser interceptada por "piratas informáticos", pero lo cierto es que estos incidentes son extremadamente raros, ya que las entidades se aseguran de encriptar sus comunicaciones. De hecho, en el Banco de España no se ha notificado nunca que la web de un banco haya sido asaltada.

En cambio, los ciberdelincuentes emplean métodos diversos para hacerse con las claves de acceso y firma electrónica de los clientes: mensajes falsos (phishing) para hacerse con nuestras claves, troyanos que espían nuestro ordenador.... ¿Cómo se aseguran las entidades de que la persona que accede a las cuentas es realmente su titular?

El DNIe mejora la seguridad en el acceso

El primer paso para operar con una cuenta bancaria es acceder a la web de la entidad financiera. Tras identificarse, normalmente el usuario puede realizar operaciones con las que se obtenga información, como consultar los saldos y movimientos, pero no puede ordenar transferencias ni traspasos, esto es, mover el dinero. En esta primera verificación de identidad se suelen emplear dos métodos: el DNIe o el nombre de usuario con contraseña.

El DNIe identifica de forma inequívoca a su propietario y equivale a su firma presencial. Sin duda, es el método de acceso más seguro porque requiere la presencia física del carnet en el lector, pero tiene un serio inconveniente: solo lo podrá utilizar desde el ordenador donde tenga instalado el certificado de usuario (vea el recuadro *Cómo se usa el DNIe)* que, normalmente, será el de su domicilio. Por tanto, este tipo de acceso le resta posibilidades y agilidad a la banca electrónica.

Todas las entidades investigadas, excepto Self Bank, ofrecen ya el acceso con DNIe electrónico.

Con usuario y contraseña, la seguridad depende de usted

La segunda modalidad de acceso a las páginas de los bancos, y la más común, es mediante un nombre de usuario asignado por la entidad o elegido por el cliente, acompañado de una clave que solo el usuario conoce.

La seguridad con este sistema depende casi enteramente del usuario: tiene que asegurarse de que nadie conoce sus claves y proteger su ordenador para que no las puedan averiguar por medio de piratería informática.

En nueve de las 14 entidades analizadas, el nombre de usuario lo determina la entidad y en todos los casos se corresponde con el DNI del cliente. En ING hay que indicar, además, la fecha de nacimiento, una seguridad adicional. Bankia también pide este dato en ocasiones, por ejemplo, cuando se ha introducido mal la contraseña en el primer intento. En Banco Popular el nombre de usuario por defecto son los 16 dígitos de la tarjeta de débito, aunque se puede modificar a voluntad. En las restantes, el nombre lo elige el cliente.

En cuanto a la contraseña,

EL DNI ELECTRÓNICO AÑADE SEGURIDAD PERO LA NECESIDAD DEL CERTIFICADO LO LIMITA A UN ORDENADOR CONCRETO

NUESTRO ESTUDIO

Para evaluar su seguridad, hemos comprobado los sistemas de verificación de la identidad que emplean los bancos más grandes del mercado y también las entidades recomendadas en alguno de nuestros análisis por la calidad de sus productos. La comprobación se ha centrado tanto en los sistemas de acceso iniciales, los que solo permiten entrar en las cuentas para consultar los saldos, como en los sistemas de firma necesarios para ordenar transferencias y mover el dinero a otras cuentas. Hemos anotado también qué entidades trabajan ya con el DNI electrónico y cuáles no.

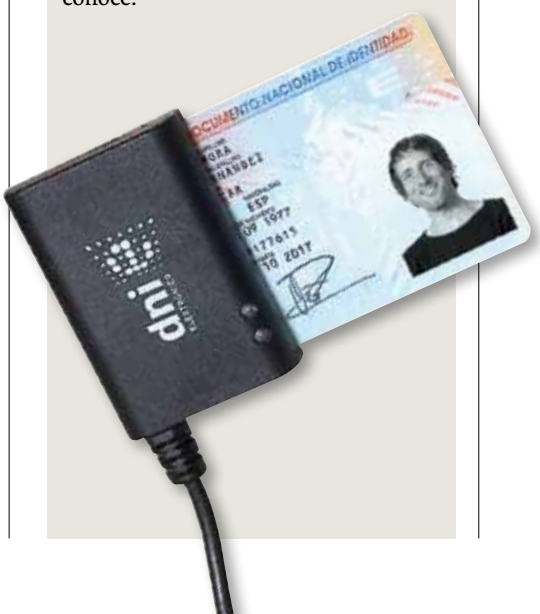
CÓMO SE USA EL DNIE

Desde 2006, el DNI lleva incorporado un chip que contiene un certificado digital. Al expedirlo, junto con el carné, se entrega una clave PIN en un sobre cerrado. Esta clave se puede cambiar en una máquina en la propia oficina de expedición.
Para poder usarlo necesita:.

- Descargar un software específico desde la página: www.dnielectronico.es/descargas/index.html. El certificado que se instala solo es válido en un ordenador.

- Instalar en su ordenador un lector de DNIe, que cuesta unos 15 euros.

Para identificarse ante una entidad, tendrá que colocar el DNI en el lector e introducir la clave que solo usted conoce.



SI QUIERE MOVER EL DINERO

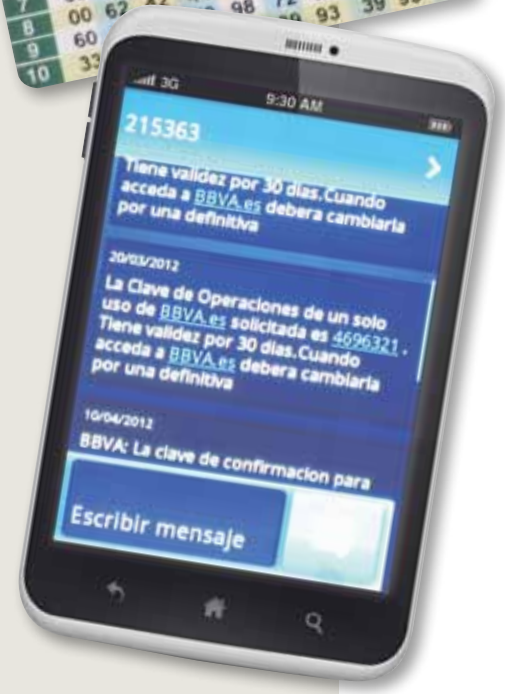
Dobles claves

Para ordenar operaciones que impliquen movimiento de dinero todas las entidades exigen una segunda verificación de identidad, la más importante para evitar fraudes. Cada entidad emplea uno o varios de los sistemas que aquí mostramos. Ninguno de ellos es en sí mismo totalmente seguro. Por eso, lo más recomendable es que se utilicen al menos dos verificaciones simultáneas: la clave de firma que conoce el cliente acompañada de la tarjeta de coordenadas o la clave aleatoria por SMS.

Clave de firma fija: es una contraseña elegida por el usuario y diferente a la que se utiliza para acceder a la web. La clave de firma es siempre la misma de manera que, si un ciberdelincuente la averigua, podrá realizar todas las operaciones que quiera.

Tarjeta de coordenadas: contienen series de números identificados por una posición. Para realizar una operación, el usuario tiene que facilitar la serie de números que corresponde a una determinada coordenada. El inconveniente de la tarjeta de claves es que tendrá que llevarla consigo si quiere operar desde cualquier lugar, con el consiguiente riesgo de pérdida.

Clave aleatoria mediante SMS: cuando se ordena una transferencia o traspaso, la entidad genera una clave de un solo uso y la envía al móvil del cliente por SMS, quien debe introducirla para validar la operación Si su banco utiliza este sistema, debe estar muy atento a no extraviar su móvil o exponerse a que se lo roben.



LOS ATAQUES A LOS SISTEMAS INFORMÁTICOS DE LOS BANCOS SON MUY INFRECUENTES: LO MÁS VULNERABLE SON NUESTRAS CLAVES

normalmente la eligen los usuarios. Bankia, BBVA y Uno-e facilitan una por defecto, que es el PIN de la tarjeta de débito, pero el usuario puede cambiarla por otra y es aconsejable que lo haga.

Y para evitar que alguien pueda dedicarse a introducir contraseñas aleatoriamente hasta dar con la buena, todos los bancos bloquean el acceso si se introduce una clave errónea tres veces seguidas. Si en alguna ocasión le ocurre esto, tendrá que ponerse en contacto con su entidad para que le facilite otra clave.

Ibercaja, la más segura

Una vez que se ha accedido a la cuenta, si quiere realizar algún movimiento de dinero, le pedirán que valide la operación con uno o más procedimientos de identificación: clave de firma, tarjeta de coordenadas o código SMS (vea el recuadro *Si quiere mover el dinero, dobles claves*). La OCU considera que es aceptable utilizar solo uno de estos sistemas de verificación pero lo óptimo es requerir al menos dos de ellos.

De las entidades analizadas, Ibercaja es la que tiene una seguridad más reforzada, pues utiliza tres sistemas de verificación: solicita la clave de firma, la coordenada de tarjeta de claves y la clave aleatoria enviada por SMS.

Otras cinco entidades emplean siempre un doble sistema de verificación. BBVA, Uno-e, Santander y Open Bank requieren la clave fija más una aleatoria enviada por SMS, mientras que ING pide una coordenada de la tarjeta de claves además de la de firma. Selfbank requiere doble identificación solo cuando se accede desde un ordenador no habitual.

En Bankia, la clave fija de firma es suficiente para rubricar cualquier operación. Las restantes entidades solo solicitan la coordenada de la tarjeta de claves.

Ahora bien, cuando se accede mediante el DNIe, algunas entidades consideran que la verificación de identidad está garantizada. En ese caso, Bankinter, BBVA y Uno-e solo piden el PIN del carnet de identidad para realizar operaciones. En los demás bancos, aunque se acceda mediante DNIe, se utilizan los mismos sistemas de comprobación que en el acceso con usuario y contraseña.

Con un tope en las transferencias

Una cautela adicional que emplean muchos bancos para evitar la captación de las claves con fines fraudulentos es el uso de teclados virtuales, diferentes del teclado físico, para

SISTEMAS DE CLAVES DE SEGURIDAD PARA E-BANCA

Entidad	Identificación del cliente para consultas					Identificación para transferencias: firma					
	Usuario	Contraseña	Segundo factor de autenticación	Teclado virtual	Acceso con DNI electrónico	Clave de firma electrónica	Coordenada de tarjeta de claves	Coordenada recibida en el móvil	Teclado virtual para introducir claves	Limite diario transferencias	Valoración
Ibercaja	✓	✓		✓	✓	✓	✓	✓	✓	no hay	98
ING Direct	✓	✓	✓	✓	✓	✓	✓		✓	30.000	92
Uno-e.com	✓	✓		✓	✓	✓ (1)		✓(1)	✓	30.000	90
Banco Santander	✓	✓		✓	✓	✓		✓		6.000	90
OpenBank.es	✓	✓		✓	✓	✓		✓		25.000	90
BBVA	✓	✓			✓	✓ (1)		✓(1)	✓	10.000	88
Selfbank	✓	✓		✓			✓	✓(2)	✓	50.000	80
Caja España Caja Duero	✓	✓		✓	✓		✓		✓	6.000	58
ActivoBank	✓	✓			✓		✓		✓	30.000	56
Banco Popular	✓	✓			✓		✓		✓	50.000	56
Bankinter	✓	✓			✓		✓ (1)		✓	50.000	56
La Caixa	✓	✓			✓		✓		✓	50.000	56
Bankia Caja Madrid	✓	✓	✓	✓	✓	✓			✓	30.000	52
Inversis	✓	✓			✓	✓				30.000	48

CÓMO LEER EL CUADRO

Identificación del cliente para consultas Resume los sistemas de verificación de identidad que se requieren para acceder a la cuenta.

Acceso con DNI electrónico Indica si la entidad oferece la opción de identificarse con DNI electrónico en lugar del usuario y la contraseña.

Clave de firma electrónica Es una contraseña que solo el usuario conoce y distinta d ela que se usa para acceder a la cuenta.

(1) Solo cuando se accede mediante usuario y contraseña, no cuando se utiliza el DNIe..

(2) Solo si se conecta desde un ordenador desconocido o se borran las *cookies*.

PARA MANTENER SU DINERO SEGURO, NO FACILITE NUNCA A NADIE LAS CLAVES DE SU CUENTA

que los usuarios introduzcan sus contraseñas. El riesgo con los teclados físicos es que se pueden seguir con programas rastreadores o *keyloggers* que se introducen subrepticiamente en nuestro ordenador y rastrean la actividad del teclado para captar nuestras contraseñas y almacenarlas en un archivo.

Y aun así, como es difícil garantizar la seguridad 100%, casi todas las entidades limitan la cantidad que se puede transferir en un solo día, que oscila entre los 6.000 euros que permiten Santander y Caja España/Caja Duero y los 50.000 que imponen las restantes. Un límite muy bajo puede ser molesto en ocasiones, pero si lo desea puede pedirle al banco que lo eleven. Solo Ibercaja, que confía plenamente en su sistema con triple verificación, no impone ningún límite a las transacciones.

Fraude: enredados o infectados

Si es usuario de banca on line, tenga presente que las técnicas fraudulentas evolucionan constantemente, aunque a grandes rasgos se clasifican en dos tipos:

> La ingeniería social, basada en engaños para que sea usted quien facilite las claves: correos que aparentan ser de su entidad, mensajes SMS, llamadas telefónicas supuestamente de su banco, incluso visitas personales...

> La infección del ordenador con virus tipo troyano o gusano, que capturan las claves. Suelen llegar camuflados en correos, archivos descargados, enlaces remitidos, etc. Ser prudente con su correo y mantener siempre actualizado su antivirus es vital para evitar esta vía de contagio.

LA OCU ACONSEJA

- **Si es posible, acceda a su cuenta con DNI electrónico: es más seguro. Una vez que se haya identificado, retire el carné del lector. Evitará que alguien averigüe su clave y pueda usarla.**
- **Si usa claves, manténgalas en secreto. No las anote en papel ni en un fichero de ordenador. Tampoco las facilite a nadie que se las pida por correo electrónico ni por teléfono.**
- **Las claves deben ser una combinación aleatoria de números y letras, que no coincidan con cumpleaños, matrículas o datos similares. Tampoco es buena idea utilizar palabras de uso común, que vienen en un diccionario.**
- **Compruebe el sistema de verificación de identidad que usa su banco. Los más seguros son los que usan un doble sistema: una clave más una coordenada o un SMS.**
- **Evite acceder a sus cuentas desde ordenadores distintos al suyo, sobre todo, si están en lugares públicos (locutorios, hoteles, bibliotecas). Procure no hacerlo tampoco a través del móvil conectado a un wi-fi público. En caso de tener que hacerlo, cambie después las claves. Antes de dejar el ordenador, cierre siempre la sesión y cierre el navegador.**
- **Mantenga actualizados el sistema operativo y el antivirus.**

LA OCU PIDE

Un protocolo de seguridad

Las entidades financieras están incentivando el uso de la banca electrónica, al tiempo que incluyen en sus contratos cláusulas en las que responsabilizan al usuario de la utilización de las claves por personas no autorizadas. Este tipo de cláusulas ya han sido declaradas abusivas por el juzgado que falló la demanda de la OCU contra varias entidades financieras. Por tanto, consideramos que deberían retirarse de los contratos. Además, la OCU va a solicitar al Banco de España y al Ministerio de Economía que imponga un protocolo de seguridad con sistema de doble verificación de identidad y la obligatoriedad de ofrecer el acceso mediante DNIe.