¿Cómo pagar con seguridad en INTERNET?

Las pasarelas de pago son seguras, pero el consumidor debe actualizar el sistema operativo de su ordenador y no transferir sus datos bancarios para que la compra on line sea un éxito

El comercio electrónico en España no crece al ritmo al que sería deseable. Entre las principales razones que los usuarios esgrimen para no comprar en la Red está el recelo a la seguridad de los sistemas de pago. HISPACOOP (Confederación Española de Cooperativas de Consumidores y Usuarios) de la que EROSKI forma parte, ha analizado los sistemas de pago y sus técnicas de seguridad con el fin de saber si son totalmente seguras. El estudio forma parte de un proyecto financiado por el Instituto Nacional de Consumo (INC) sobre el comercio y la contratación electrónica. La principal conclusión ha sido que el talón de Aquiles de la compra no está en los sistemas, completamente seguros, sino en las cautelas del usuario a la hora de dejar sus datos en páginas no fiables, y en la falta de cuidado del ordenador. Para asegurar al máximo la compra on line, los expertos que han elaborado este estudio han creado un detallado protocolo de actuación que detecta el fraude, valora la seguridad de los comercios y mantiene el ordenador libre de programas espía. Si se siguen los consejos dictados a continuación, el riesgo de sufrir problemas en el apartado de la seguridad en los pagos realizados en Internet se reducirá de manera notable.

Siempre que el usuario compra en un comercio on line selecciona el producto o servicio a comprar, especifica el número de unidades del mismo y pulsa el botón de "ir a la página de compra". De este modo, llega a una página donde se le pide que deje algunos de sus datos personales -nombre, apellidos, documento nacional de identidad, teléfono de contacto, etc.-, así como los datos de su tarjeta de crédito o débito. El comprador rellena entonces los campos requeridos, escribe los datos de su tarjeta y pulsa el botón de "ejecutar la compra". A partir de ahí, pierde el control de la información que ha depositado.

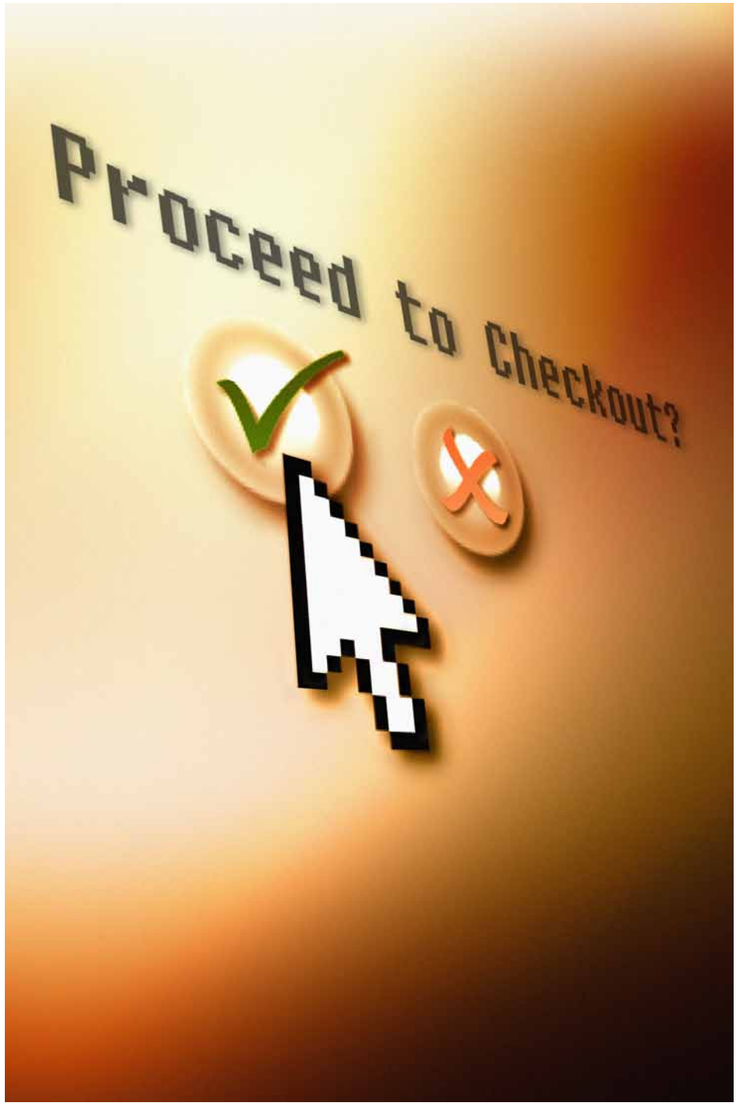
¿Significa esto que un peligro inminente de robo, uso fraudulento o estafa acecha al usuario? Desde luego no desde el punto de vista técnico. Al menos hasta que no se demuestre lo contrario, y todavía no se ha hecho. Los sistemas de pago más usuales en la Red son totalmente seguros. Es decir, ningún "ciberdelincuente" puede colarse en la operación de pago ni robar las claves de la tarjeta y las cuentas del usuario mientras viajan desde la página de pago al comercio. Esto es válido siempre que se cumplan una serie de supuestos: que el comercio no actúe de mala fe -algo que también puede suceder en los establecimientos físicos- y que el sistema de pago, también llamado pasarela, que use ese comercio sea un protocolo seguro SSL (Secure Lay Shocked-Protocolo de capa de conexión segura).

Y SIN EMBARGO NOS ENGAÑAN.

Ahora bien, muchas personas pensarán: *"pues yo he leído en prensa sobre casos de uso fraudulento de tarjetas*

Los sistemas de pago más comunes en la Red son totalmente seguros

Los métodos de engaño de los ciberdelincuentes no son técnicos sino psicológicos



de personas que habían realizado compras en Internet". Incluso puede que alguna de estas personas haya experimentado en sus propias carnes esta mala experiencia. ¿Dónde está el problema si los sistemas son infalibles? Por un lado, aunque no sirva de excusa, hay que matizar que estos casos son poco habituales a pesar de la exagerada resonancia mediática que adquieren. Por otro, se debe asumir que toda compra tiene su punto débil en la actitud del usuario. No se trata de culpar al comprador, por descontado, sino de hacerle consciente de que la seguridad de la compra depende en un 99% de él mismo.

Los ciberdelincuentes existen y están siempre al acecho, pero sus métodos de engaño no son técnicos sino psicológicos. Juegan con las debilidades, deseos y miedos de las personas para conseguir sus claves bancarias. Son grandes expertos, pero no en técnicas de cifrado o informática, sino en psicología humana. Para empezar, no llegan al usuario con las mismas artes que los comercios serios.

Estos ladrones de última generación acceden al usuario por medio de correos electrónicos no deseados que superan los filtros de spam -aunque cada vez son menos los que lo consiguen-, y que engatusan al internauta para que abra un archivo que le instalará un programa espía en el ordenador. O bien le incitan a pinchar en un enlace que lleva a una página web falsa con el fin de ofrecerle diversos productos a precio muy reducido o difíciles de encontrar en el país. Otras veces su táctica consiste en dar una falsa alarma al usuario para que mediante una dirección URL que le ofrecen entre en una página falsa de su banco y deje sus claves.

Los ciberdelincuentes saben que en la mayoría de las ocasiones fracasarán en su intento y serán descubiertos. Pero también es cierto que un pequeño porcentaje de personas caerá en la trampa y se dejará robar sus cuentas bancarias o tal vez, pagará un dinero por el que no recibirá nada a cambio. Como el esfuerzo que realizan es mínimo y su estafa llega a cientos de miles de buzones, con unos pocos incautos que muerdan el anzuelo es fácil recuperar la inversión.

PROTOCOLO DE ACTUACIÓN

1. Aprender a defenderse del fraude

La primera medida para que esto no suceda es que el usuario aprenda a defenderse de las estafas. Sus datos bancarios son intransferibles y debe fijarse con detenimiento dónde los escribe. Como norma inquebrantable, nunca se debe abrir un correo electrónico que no se haya pedido expresamente o que tenga un remitente desconocido. Ni bancos ni cajas ni servicios de pago, como PayPal y otros, envían mensajes de correo para pedirle que entre en su página, ya sea para probar nuevos servicios o para alertar de algún problema. No lo hacen jamás y en el caso de que lo hagan nunca le ofrecerán una dirección URL dentro del correo para que entre en el servicio. Le dirán, sin embargo, que lo haga siempre desde la barra del navegador. En resumen, no hay que entrar nunca en una página web desde un correo electrónico que resulte sospechoso o que no se haya pedido. Este tipo de emails debe ser remitido, sin abrir, a la carpeta de spam.

En caso de que un internauta abra uno de estos correos de manera accidental y acceda a la dirección web que se le propone en un enlace, y en la que se le ofrece algún producto en venta o se le pide que deje sus datos, jamás debe comprar o escribir ningún dato. Es fácil comprobar que se trata

de una cuenta falsa: basta con mirar primero la dirección del remitente del spam y verá que no se corresponde con la de ninguna empresa conocida sino que es de un particular. Además, en la página web que le proponen, el consumidor comprobará que la dirección URL no pertenece a empresa alguna, sino que es una larga lista de letras y números sin significado alguno. Es la primera prueba de que la página es falsa.

Si el usuario llega a una página donde se le pide dejar sus datos o efectuar la compra del producto que le ofrecen, podrá comprobar fácilmente que no está en un sistema SSL. Lo sabrá, en primer lugar, porque la dirección URL de la página no es «https» (todas las SSL lo son) sino «http», y por lo tanto no es una página segura. Con este dato debería bastar, pero es mejor seguir la comprobación y buscar un candado en la parte inferior derecha del navegador (no del sitio web, sino del navegador). Si no existe, no hay que buscar más: la página es un fraude.

Para completar la comprobación se puede pinchar en la cabecera que antecede a la casilla de la dirección URL en el navegador. Al hacerlo, si la página es SSL, aparecerá la certificación del navegador, que explicará en una ventana emergente los protocolos de cifrado empleados, así como la empresa de seguridad que verifica el protocolo. Las empresas de seguridad jamás responden por páginas fraudulentas. Si la página lo es, el

■ Para mantener el ordenador libre de amenazas es fundamental actualizar el sistema operativo

■■■ navegador lo hace saber al pinchar en la cabecera, ya que en su ventana emergente anunciará que la página no está cifrada y los datos que se dejen en ella pueden ser usurpados por terceros. Por lo tanto, y tras comprobarlo, nunca se debe comprar en páginas que no utilicen protocolos SSL para realizar los pagos.

2. Comprar en un entorno seguro

Pero más allá de prevenirse contra los fraudes, el comprador debe extender su cautela a la propia ubicación del comercio, porque no es lo mismo comprar de forma on line en España, Francia o Inglaterra que hacerlo en otro país remoto y de dudosa reputación. Hay que ponderar dónde se compra y la seriedad del comercio. Este debe tener a disposición del usuario un servicio de atención al cliente con una dirección de correo electrónico y un teléfono, además de otros posibles sistemas. Otra muestra de tienda segura es que en las condiciones del contrato o en el apartado "quiénes somos" se muestre información veraz y contrastable sobre el domicilio social de la empresa y sus titulares.

Además, debe especificar a qué legislación se acoge y confirmar que cumple con la Ley de Protección de Datos del país al que pertenezca. No está de más que explique los protocolos de seguridad que utiliza para almacenar los datos de los particulares. Estos indicadores se encuentran en los servicios y tiendas de la mayoría de países del entorno de la Unión Europea, Estados Unidos, Canadá. Corea, Japón, Brasil o China. Sin embargo, en otros países también puede haber negocios serios y eficaces. Si cumplen los indicadores especificados, ofrecen buenas garantías. Como norma es preferible comprar en tiendas grandes y de marcas globales, entre otras razones porque a la hora de reclamar será más difícil que puedan esquivar sus responsabilidades.

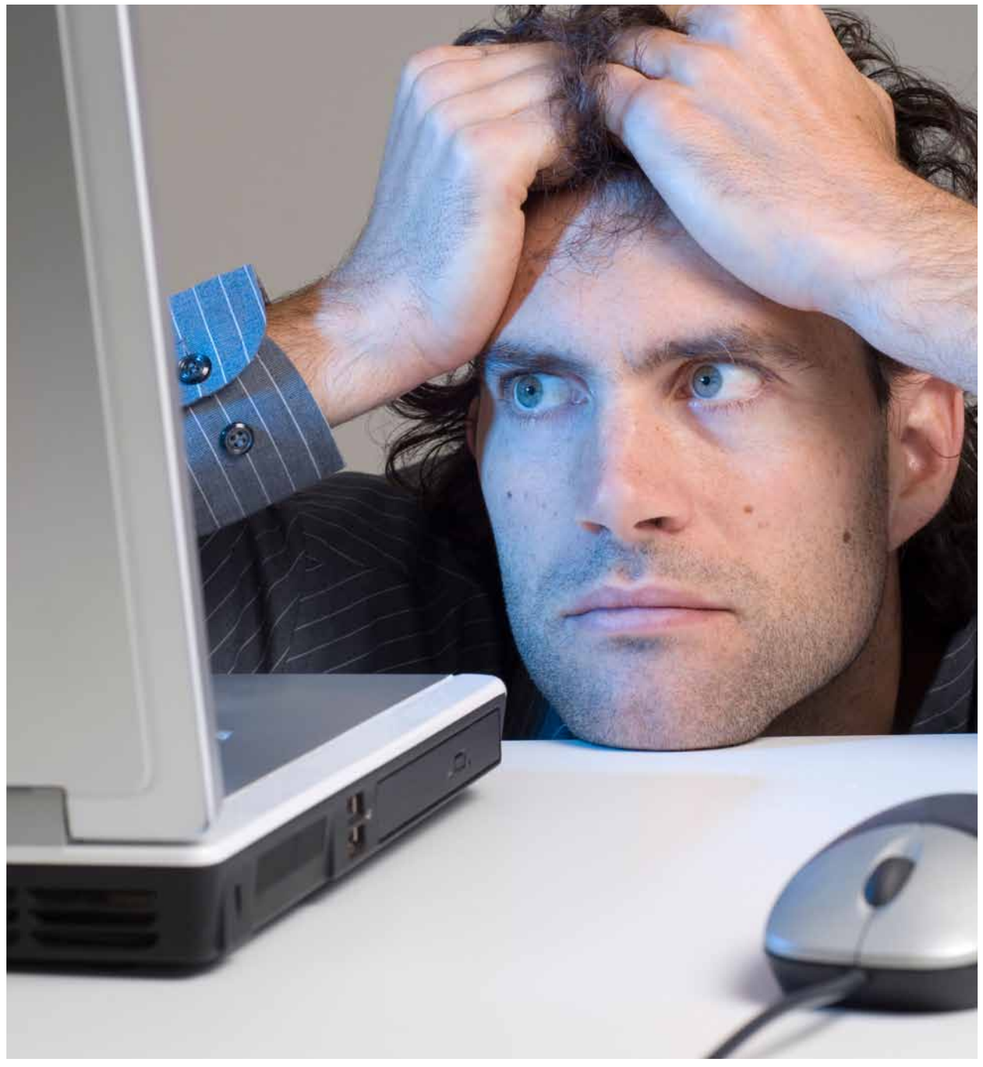
3. Mantener el ordenador limpio

Y por último, aunque no menos importante, se debe mantener el equipo informático limpio, sobre todo quienes usen cualquiera de las versiones del sistema operativo Windows. Aunque los ataques por programas espías -conocidos como troyanos- son los que menor incidencia tienen, la falta de prevención y cuidados facilita su entrada.

En primer lugar hay que mantener siempre el sistema operativo actualizado. Windows actualiza periódicamente sus principales versiones para corregir vulnerabilidades. Es fundamental asegurarse de tener un cortafuegos instalado en el ordenador y de que esté actualizado y activado de manera constante, además de contar con un sistema antivirus activado y actualizado. Por otro lado, se deben usar periódicamente programas que limpian el ordenador. En la Red se pueden encontrar muchos tanto de pago como gratuitos. Para terminar, es conveniente mantener el navegador siempre actualizado con la última versión que se haya lanzado a la Red. ■

MÁS INFORMACIÓN

www.consumer.es



SSL, un método infalible

SSL, o "Secure Lay Socked", hace referencia a un proceso que convierte los datos de la tarjeta del comprador en complejas claves alfanuméricas para, más tarde, enviarlas cifradas al comerciante. Una vez allí, éste las pasa a la entidad de crédito o banco del usuario y reclama el pago. La entidad confirma que la petición es válida y realiza la transferencia. Todo este proceso se desarrolla de manera automática entre servidores equipados con la mayor seguridad, y **en cada envío se descifran los datos para leerlos y se cifran de nuevo**. La duración de esta operación es de aproximadamente cuatro segundos.

En los servidores, tanto del banco como del comercio, y en cada envío, los datos se mantienen en clave con dos tipos de cifrado, uno asimétrico y otro simétrico. **El cifrado asimétrico**, generalmente conocido como **RSA**, es un complejo sistema que funciona como una valija diplomática donde se albergan los datos del usuario, de nuevo cifrados con un algoritmo (sistema) simétrico. El cifrado RSA funciona con una clave pública y otra privada. La pública sirve para realizar el cifrado de los datos, y la privada es la única que puede descifrarlos. De este modo, cuando un comprador pone sus datos en una página de pagos que usa el protocolo SSL, usa sin saberlo y de forma automática, la clave pública para crear una caja de cifrado asimétrico. Dentro de esta caja, **el sistema SSL usa un cifrado simétrico de alta complejidad** para cifrar los datos. Así, con este doble cifrado, son enviados a los servidores del banco y del comercio. Allí residen las claves privadas para descifrar el asimétrico y abrir la caja, y después descifrar el simétrico.

Respecto a la seguridad de este sistema basta decir que los mayores expertos del mundo auguran que el cifrado asimétrico RSA podrá romperse -ser atacado- cuando se invente el **ordenador cuántico**, algo muy lejano todavía y que sería imposible de llevar a cabo con los ordenadores actuales. En cuanto al simétrico, se utilizan sobre todo dos niveles de complejidad de las claves. El primero es el RC4 128 bit, que está definido como estándar por el gobierno de los Estados Unidos para guardar su información sensible.