TRANSACCIONES ONLINE: CUESTIÓN DE SEGURIDAD Y DE CONFIANZA.

Rafael Martínez Benito.

Profesor técnico de sistemas y aplicaciones informáticas desde 2001. Diplomado en Estadística. Licenciado en Técnicas e Investigación de Mercados. Cursos de doctorado perteneciente al programa Dirección de Empresas y Gestión de Marketing III. Autor del trabajo de investigación del programa de doctorado: Marketing de relaciones; Gestión de las Relaciones con los Proveedores y Cultura Organizacional.

Es habitual tener miedo cuando vamos a montarnos en un avión, menos habitual es tenerlo cuando nos montamos en un coche; sin embargo estadísticamente está probado que tenemos mas posibilidades de tener un accidente cuando subimos a un coche que cuando lo hacemos a un avión, por tanto no se trata tanto de un problema de seguridad como de confianza. Si trasladamos esto a las operaciones monetarias online, la inseguridad que siente mucha gente a la hora de hacer una transacción monetaria por Internet es también un problema de confianza y no tanto de seguridad. Según nos muestran nuevamente las estadísticas es más probable sufrir un atraco en un cajero o a la salida de un banco que a través de la red.

El miedo a volar es quizás inevitable ya que sentimos que es un medio antinatural para nosotros, pero puede que no ocurra lo mismo con Internet, sentimos desconfianza hacia la red porque no sabemos como funciona ni cuales son sus medidas de seguridad y no por su supuesta inseguridad, seguimos confiando más en los métodos de siempre: la oficina y más recientemente los cajeros. Pero si echamos la vista atrás, también antes la gente era más reacia a utilizar los cajeros automáticos para sacar dinero y aun hoy en día la gente mayor sigue sin utilizarlos. ¿Ocurrirá lo mismo con Internet? Es de esperar que sí, de hecho la gente más joven es la que realiza, con diferencia, más transacciones monetarias con este método.

Pues bien, con este artículo pretendemos dar pistas para que cuando nos sentemos delante de nuestro ordenador y vayamos a realizar una transacción monetaria nos sintamos más seguros. Si lo conseguimos, aunque sea en pequeño grado, daremos por conseguido el objetivo del artículo.

Cuando se trata de prestar dinero o de confiar un objeto o un ser querido a alguien optamos por aquellas personas o estamentos en los que tenemos más confianza por su trayectoria o por el conocimiento que tenemos de ellos en experiencias anteriores. Existe otra posibilidad, la de confiar en aquellas personas o entidades que nos garanticen de alguna manera la seguridad de lo que entregamos.

Pues bien, se trata de hacer lo mismo cuando operamos en Internet. Por un lado tendremos que tener presente con quien estamos realizando la operación, es obvio que si conocemos la empresa o hemos realizado anteriormente operaciones con ella y no hemos tenido problemas, nuestra seguridad en que todo va a ir bien será mayor. Por el contrario no es nada recomendable hacer ningún tipo de operación monetaria con aquellas páginas que no sepamos quienes son sus creadores ni a quien pertenecen y que no hayamos oído hablar nunca de ellas. Este sería el primer consejo: no hacer ninguna transacción con "desconocidos".

La otra vía que nos puede dar mayor seguridad y confianza a la hora de operar en Internet viene de la garantía que nos ofrecen ciertos estamentos de que un sitio web es seguro. En este caso se trata de confiar en ciertos organismos oficiales y en los expertos que nos garantizan que ciertos sitios web cumplen con unas determinadas normas de seguridad que garantizan la confidencialidad y seguridad de nuestros datos y transacciones monetarias.

SSL (Secure Sockets Layer) es un protocolo diseñado por la empresa Netscape para realizar comunicaciones encriptadas en internet. Es decir, consta de una serie de normas para encriptar la información de manera que ésta se convierta en información segura. SSL da privacidad a los datos y mensajes, además permite autentificar (verificar la identidad de una persona, usuario o proceso, para así acceder a determinados recursos o poder realizar determinadas tareas) los datos enviados.

Por otro lado VeriSign es una empresa estadounidense con sede en Mountain View, California, fundada en 1995 y que se encarga de un diverso conjunto de infraestructuras de red, incluyendo una variedad de servicios de seguridad y telecomunicaciones desde certificados digitales, procesos de pagos y gestión de cortafuegos, etc.

VeriSign se encarga de emitir los certificados digitales que garantizan transmisiones seguras realizadas con el protocolo SSL, especialmente para la protección de sitios web.

Es decir, nos garantiza que un sitio web cumple con una serie de medidas de seguridad que han sido previamente auditadas y que al cumplir dichas medidas nuestros datos y transacciones están protegidos según unas normas específicas de seguridad.

Queda saber qué sitios cumplen con esas medidas y por tanto tienen concedido dicho certificado digital. Es bien fácil, basta con mirar en la barra de direcciones y si en lugar de aparecer http (Hypertext Transfer Protocol o protocolo de transferencia de hipertexto) aparece https (Hypertext Transfer Protocol Secure o protocolo seguro de transferencia de hipertexto) estaremos ante un sitio seguro que tiene concedido el certificado digital y que por tanto cumple con las normas de seguridad establecidas. Todos los bancos que se precien de ser mínimamente seguros y muchas empresas que operan en Internet utilizan este certificado.

Otra pista para saber que estamos en un sitio seguro es el candado amarillo que aparece situado en la barra de abajo del navegador Internet Explorer y en algunos casos en la propia barra de direcciones. Su presencia significa que el navegador está enviando y recibiendo información codificada. Esto implica es que estás navegando dentro de una zona segura.

Estos sistemas de protección son bastante eficaces y su historia está ligada en gran medida a nuestro país. Para darnos una idea de ello os contamos la trayectoria de uno de los mayores expertos en seguridad y de las consecuencias de sus trabajos.

En 1988 Carlos Jiménez estudiante de informática crea el primer antivirus de la historia contra el virus "Viernes 13". El Ministerio de Economía y Hacienda lo distribuye a más de 100.000 empresas.

En 1990 crea Anyware, primera empresa europea de I+D+i en Seguridad Informática. El antivirus Anyware recibe el premio PC World al mejor producto del año.

En 1996 Anyware es el segundo antivirus más descargado de internet (200.000 copias al mes).

En 1998 Carlos Jiménez vende Anyware a McAfee y funda Secuware para dar respuesta más amplia a los nuevos retos en Seguridad Informática. Desarrolla tecnología de cifrado para el Ministerio de Defensa bajo la dirección del Centro Nacional de Inteligencia. Secuware es considerada empresa de interés estratégico nacional.

En 1999 se crea cypt2000 un programa de seguridad contra terceros, certificado por el Ministerio de Defensa Español conforme a la Ley Orgánica de Protección de Datos de Carácter Personal.

Crypt2000 se convierte en software estrella en los sistemas de seguridad:

- ✓ Garantiza el control de acceso y preserva la confidencialidad de la información contenida en los PC's.
- ✓ Ofrece una seguridad total de la información, para ello cifra por completo el disco duro, incluyendo el sistema operativo.
- ✓ Es independiente de los programas, dispositivos y ficheros que contenga el PC.
- ✓ Introduce mecanismos de seguridad para proteger los datos de posibles alteraciones no deseadas (virus, caballos de troya,...) y de accesos de lectura no autorizados.
- ✓ Garantiza la protección total del acceso a PC's desde el momento del encendido de éstos.
- ✓ Opera en diferentes plataformas de sistema operativo.
- ✓ Permite manejar tarjetas inteligentes que contienen certificados digitales o utilizadas como medio de pago en el comercio electrónico.
- ✓ Mediante el cifrado de dispositivos (IDEA), evita el robo de información vital supervisando todo dato que entra o sale de los PC's.

Desde que creara el primer antivirus de la historia con apenas 20 años, hasta la actualidad, en la que es fundador y presidente de Secuware, Carlos Jiménez se ha convertido en una autoridad mundial en seguridad informática y experto en ciberterrorismo, reconocido por organizaciones como la OTAN, el Ministerio de Defensa o el CNI.

A continuación se enumeran las empresas y organismos que en nuestro país utilizan la solución de seguridad cript2000:

- Banca y seguros
  - BBVA
  - Caja de Madrid

    - Caixa de Catalunya
    - Banco de España
    - Mapfre
- Distribución
    - El Corte Inglés
- Informática
    - Microsoft
    - Informática el Corte Inglés
    - IBM
    - Compaq
    - Bull
    - SIA
    - ACE

- Administración Publica
    - Agencia Tributaria
    - Mº de Defensa
    - Mº de Presidencia y Presidencia del Gobierno
    - Fábrica Nacional de Moneda y Timbre
    - Dirección General de la Policía
    - Guardia Civil
    - Estado Mayor del Ejército
- Telecomunicaciones
    - Ono
    - Telefónica Corporación
    - Telefónica Data
    - Vodafone
- Electricidad y Transporte
    - Iberdrola
    - Red Eléctrica de España
    - Metro de Madrid

Por último, y para hacernos una idea de los niveles de seguridad de estos sistemas, os contamos, en torno a crypt2000, una anécdota, que no por ello deja de ser real. Cuando se creó dicho sistema de encriptación, el fundador de Secuware lanzó un reto: quien fuera capaz de violar el sistema creado por su empresa, él mismo se comprometía a pagarle un millón de euros, pues bien, durante el tiempo que estuvo vigente dicho reto (aproximadamente dos años) nadie pudo conseguir violar el sistema y por tanto nadie consiguió el dinero.

Para terminar y dado que los cacos cibernéticos saben todo esto e intentan aprovecharlo con técnicas como el phising (filtro de suplantación de identidad), programas espías, etc., es necesario tener instalados en nuestros equipos sistemas de seguridad que eviten los ataques de dichos cacos.

Como hemos dicho antes, la confianza en el sitio web es fundamental a la hora de decidirnos a operar en Internet, pero ¿quien nos garantiza que al otro lado está quien realmente dice ser?. El phising es una técnica que consiste en la suplantación de identidad en línea, es una forma de engañar a los usuarios para que revelen información personal o financiera a través de un mensaje de correo

electrónico o sitio web. Normalmente, una estafa por suplantación de identidad empieza con un mensaje de correo electrónico que parece un comunicado oficial de una fuente de confianza, como un banco, una compañía de tarjeta de crédito o un comerciante en línea reconocido. En el mensaje de correo electrónico, se dirige a los destinatarios a un sitio web fraudulento, donde se les pide que proporcionen sus datos personales, como un número de cuenta o una contraseña. Después, esta información se usa para el robo de identidad.

Por otro lado un programa espía, traducción del inglés spyware, es un software que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en el. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.

Para protegernos de todo ello es necesario, por tanto, la instalación en nuestro equipo de un paquete de seguridad eficaz; existen una gran cantidad de ellos cuya calidad ha sido suficientemente contrastada en el mercado. Estos paquetes deben contener herramientas como antiphising y antispyware para eliminar los peligros anteriormente mencionados además de antivirus, cortafuegos o sistemas de protección de identidad.

Siguiendo los consejos anteriores creemos que los usuarios de Internet que con mayor o menor asiduidad realizan transacciones monetarias se sentirán algo más seguros al realizar dichas operaciones y aquellos que todavía siguen desconfiando de la red de redes se animen a utilizar un medio más cómodo, rápido y ¿por que no?, seguro.