



Consejos para
una navidad
segura



INDICE

1. <i>Introducción</i>	3
2. Riesgos en la Red: Amenazas para una compra segura.....	3
3. ¿Cómo debe ser una página de comercio electrónico segura?.....	4
4. ¿Qué medidas de seguridad deben adoptar los usuarios?.....	5
5. Conclusiones: consejos básicos para operar con seguridad en Internet.....	7

1. Introducción

Cada vez son más los que deciden buscar en Internet ese regalo original o divertido que desean regalar estas navidades. La red se ha convertido en un inmenso escaparate en el que se puede encontrar prácticamente de todo y, muchas veces, a precios más bajos.

Sólo en España, las transacciones online alcanzaron durante 2007 los 3.740 millones de euros, un 52% más que en 2006¹. De cara al 2009, la consultora Forrester prevé un crecimiento mundial de las transacciones online del 12,2%².

Los delincuentes de la Red no suelen atacar directamente a las empresas, sino que dirigen sus esfuerzos contra el eslabón más débil de la cadena: el propio usuario. Así, para un ciber-criminal es más fácil obtener datos confidenciales desde un PC particular que intentando "colarse" en un servidor para robar una base de datos o interceptar comunicaciones que en muchos casos se encuentran cifradas.

A continuación, veremos los riesgos que amenazan a los usuarios en Internet y las medidas de seguridad que deben cumplir tanto el negocio online como el usuario, para conseguir la máxima seguridad en las compras online.

2. Riesgos en la Red: Amenazas para una compra segura

Troyanos bancarios: se trata de códigos maliciosos diseñados para robar los datos bancarios de los usuarios. Estos troyanos pueden llegar como archivo adjunto en un correo, haciéndose pasar por una descarga legítima en programas como el eMule o Ares, visitando ciertas páginas web, etc. Generalmente, son muy silenciosos, de tal modo que un usuario puede estar infectado con uno de estos ejemplares y no percatarse, ya que su ordenador seguirá funcionando con normalidad. Cuando el usuario visite su banco estos troyanos capturarán las contraseñas que introduzca, su número de cuenta, etc. Puede obtener más información sobre los troyanos aquí. <http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/trojan/>

Spam: Se conoce como spam a los correos electrónicos no solicitados, es decir, aquellos que llegan a nuestra bandeja sin que sepamos de quien procede. Generalmente, anuncian algún tipo de producto. Por muy atractiva que pueda parecer una oferta, el hecho de provenir de una fuente dudosa ya debe despertar recelo. ¿Estamos seguros de que se trata de un auténtico vendedor o se trata de un delincuente que sólo trata de estafar a los usuarios vendiendo productos que nunca enviará? O aún peor, ¿ese spam no tendrá como objetivo conseguir nuestros datos bancarios para realizar estafas online y vaciarnos la cuenta corriente o el crédito de la tarjeta? Además, en caso de llegar, esos productos pueden ser peligrosos o estar defectuosos.

Phishing: Es una modalidad de correo electrónico no deseado que por norma general aparenta provenir de comercios online o entidades financieras. Habitualmente se presentan ante el usuario con la excusa de algún problema informático, y solicitan confirmar sus datos. Según el Grupo Centro de Cooperación Interbancaria CCI-Seguridad Informática, el fraude en banca online mantiene una tendencia al alza que se encuentra entre un 10% a un 20% anual.

Falsas tarjetas navideñas: Un clásico de las navidades, en lo que a malware se refiere, son las falsas tarjetas navideñas. Se trata de correos electrónicos en los que se ofrece al usuario descargarse una tarjeta navideña online que le ha enviado, supuestamente, un amigo. Cuando lo haga, realmente estará introduciendo en su equipo algún tipo de malware.

Tiendas online falsas: Se trata de páginas que simulan ser tiendas online legales. En ella se anuncian productos de todo tipo, generalmente, a precios muy suculentos, para así atraer a los

usuarios. Por norma general, estas tiendas están diseñadas para robar los datos bancarios de los usuarios que compran en ellas. Éstos nunca llegan a recibir producto alguno.

Falsas subastas: Otra técnica utilizada por los ciberdelincuentes de la red, aunque aún no tan extendida como las anteriores. Consiste en incluir comentarios en páginas de subastas como eBay haciéndose pasar por los vendedores legítimos de un producto u ofertando otro similar e invitando al usuario a visitar cierta página web en la que se le ofrecerá un producto muy rebajado. En realidad, el propósito vuelve a ser hacerse con los datos del usuario.

3. ¿Cómo debe ser una página de comercio electrónico segura?

Las páginas web en las que realicemos transacciones monetarias online deben cumplir una serie de requisitos técnicos para garantizar la seguridad de los usuarios. Son los siguientes:

- Tienen que garantizar que los datos introducidos para realizar la transacción sólo sean accesibles a las partes implicadas en la misma, lo cual puede hacerse cifrando esa información.

- Deben mantener la integridad de la información durante toda la operación, de forma que no puedan ser manipulados. Esto se consigue con el empleo de firmas digitales.

- Finalmente, tienen que verificar la identidad tanto de la parte compradora como de la vendedora, lo cual se logra mediante la emisión de certificados digitales.



Para conseguir esto, se han desarrollado protocolos de seguridad para comercio electrónico que cumplen, totalmente o en parte, estos requisitos.

3.1. Protocolos de seguridad

Un protocolo de seguridad no es ni más ni menos que un conjunto de especificaciones desarrolladas para conseguir una manera segura de realizar transacciones electrónicas, procurando el cumplimiento de los requisitos antes mencionados. En ellas están involucrados el usuario final, el comerciante, las entidades financieras, las compañías administradoras de tarjetas y los propietarios de las marcas de tarjetas.

El sistema de transacciones seguras más utilizado en la actualidad se basa, principalmente, en el protocolo de seguridad SSL (Secure Socket Layer). Éste se encarga de **cifrar** los datos introducidos y de **descifrarlos** cuando llegan a su destino. De esta forma, aunque una tercera persona interceptase los datos, no podría acceder a ellos sin una clave capaz de descifrar la información. En este protocolo, tan sólo el vendedor muestra un certificado digital que verifica su identidad, cosa que no hace el comprador.

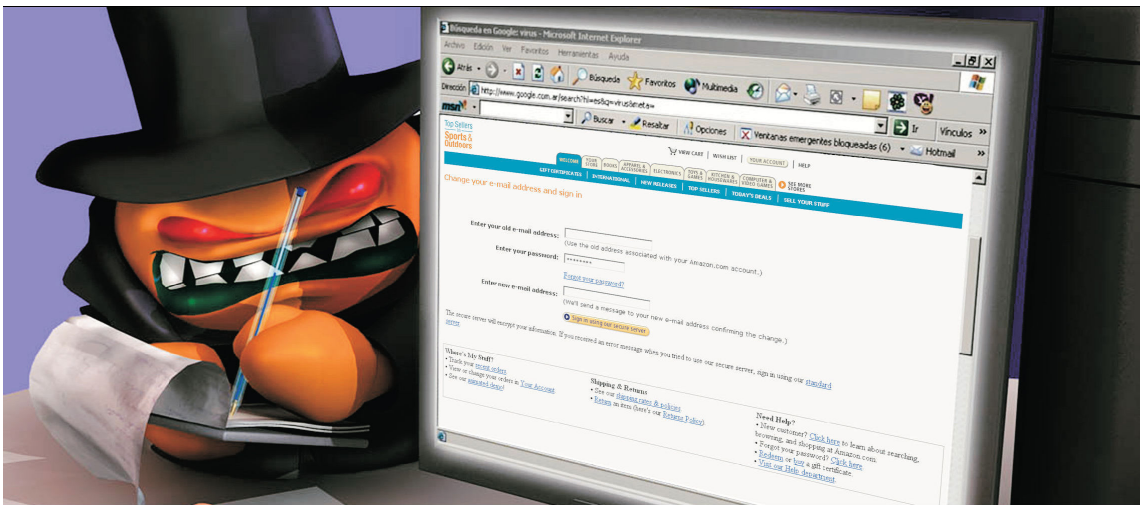
3.2 Certificación del servidor

Además de emplear un sistema de transacción seguro, cualquier empresa de comercio electrónico que se precie ha de tener la certificación de seguridad para sus servidores otorgada por alguna autoridad certificadora reconocida. Realmente, en este aspecto, no hay mucha diferencia con el comercio tradicional ya que, al igual que nadie daría sus datos a la primera persona que intentase venderle algo, tampoco debería introducirlos en servidores que no

tengan esta certificación. Por otra parte, la empresa también debe cuidar que sus servidores estén totalmente libres de virus o de troyanos para preservar integridad de los datos que poseen. De hecho, algunos de estos virus y troyanos son introducidos en los sistemas informáticos con el único objetivo de provocar vulnerabilidades en los servidores de tal forma, que permitan a un hacker realizar distintas acciones, como puede ser la extracción de una base de datos de clientes.

Las autoridades certificadoras se encargan de verificar que el servidor es capaz de soportar el protocolo de seguridad. Asimismo, se ocupan de expedir los certificados digitales a empresas o compradores.

Existen varias autoridades de certificación; de ellas Verisign es la más conocida internacionalmente.



4. ¿Qué medidas de seguridad deben adoptar los usuarios?

Antes de hacer una compra online o de acceder a un servicio bancario de Internet es básico asegurarse de que no existe ningún virus instalado en el ordenador que se encuentre activo en ese momento. En este sentido los más comunes, y también los más peligrosos, son los troyanos bancarios que permanecen a la espera de que el usuario se conecte a determinadas páginas bancarias, sistemas de pago tipo Pay Pal o tiendas virtuales, para capturar y enviar al delincuente los datos confidenciales que el usuario introduce para realizar la transacción.

Por ello, es fundamental disponer de una solución de seguridad perfectamente actualizada. Pero eso no es todo, en la actualidad nos encontramos en una nueva dinámica del malware, en la que los delincuentes tratan de poner en circulación muchos virus que se instalan de forma silenciosa. Con ello, pretenden que las compañías de seguridad no se percaten de su presencia y, por tanto, no puedan neutralizarlos. Así, es necesario **complementar las soluciones de seguridad tradicionales con tecnologías proactivas capaces de detectar amenazas por sí mismas analizando su comportamiento**, y sin necesidad de conocerlos con anterioridad.

Además, **es muy conveniente utilizar herramientas de “segunda opinión”**. Dado el enorme volumen de nuevas amenazas que aparecen cada día, los laboratorios de seguridad muchas veces no dan abasto, y esto provoca que no todos los antivirus detecten lo mismo. Debido a ello, es muy recomendable analizar el equipo con un antivirus capaz de detectar más malware que otras soluciones. Panda Security dispone de una herramienta a tal fin, **Panda ActiveScan**, que pueden utilizarse gratuitamente en la dirección <http://www.pandasecurity.com/activescan>

Nunca hay que hacer caso a los mensajes de spam publicitarios ni a los correos que digan proceder de entidades bancarias, pues, como ya hemos visto, se tratará de intentos de **phishing**. Hay que tener en cuenta que ninguna entidad se pondrá en contacto con el usuario para pedirle sus datos personales y/o confidenciales. De todas formas, **en caso de duda, antes de introducir ningún dato, póngase en contacto con el banco donde le confirmarán la veracidad del asunto.**

Por supuesto, **nunca pulse sobre ningún link que aparezca en dichos mensajes**, ya que conducen a páginas que, aunque imitan a los originales, no tienen nada que ver con la tienda o banco en cuestión, y su cometido es robar los datos personales que introduzca en ellas.

Antes de comprar en un comercio online, o en una web de subastas, por ejemplo, es muy recomendable investigar un poco en Internet sobre la reputación del vendedor. De esa manera, podrán evitarse desagradables sorpresas en forma de timadores.

Mantenga siempre actualizado su sistema. Muchas veces las aplicaciones o el sistema operativo que tenga instalado en su PC tienen vulnerabilidades que pueden servir para instalar códigos maliciosos o introducirse en el ordenador sin que el usuario se de cuenta de ello. No importa cual sea la aplicación: un problema de seguridad en un reproductor de música puede servir.

La mejor manera de estar siempre al día es utilizar la opción de actualizaciones que suelen incluir la mayoría de las aplicaciones o mantenerse informado sobre las noticias de seguridad más recientes.

No ejecute nunca archivos que no provengan de fuentes fiables, como adjuntos a mensajes de correo electrónico sospechosos, o descargados desde páginas web de contenido dudoso. Piense que con ello puede estar instalando un virus en su ordenador.

No pague nunca nada sin estar totalmente seguro. El timo en Internet es

mucho más frecuente de lo que parece. No sería la primera persona que compra un móvil de última generación y a cambio recibe una caja con piedras en su interior.

Si se trata de un artículo sobre el que está pujando en una web de subastas, desconfíe de las ofertas que algunos delincuentes, haciéndose pasar por el vendedor del producto, puedan hacerle a través de correo electrónico con la excusa de conseguirle un mejor precio, o una mayor rapidez en la transacción.



The image shows a screenshot of an email from the Federal Reserve Bank System Administration. The header features the Federal Reserve Bank logo and the text "FEDERAL RESERVE BANK". The main body of the email is titled "Important:" and contains the following text: "You're getting this letter in connection with new directions issued by U.S. Treasury Department. The directions concern U.S. Federal Wire online payments. On November 3, 2008 a large-scaled phishing attack started and has been still lasting. A great number of banks and credit unions is affected by this attack and quantity of illegal wire transfers has reached an extremely high level. U.S. Treasury Department, Federal Reserve and Federal Deposit Insurance Corporation (FDIC) in common worked out a complex of immediate actions for the highest possible reduction of fraudulent operations. We regret to inform you that definite restrictions will be applied to all Federal Wire transfers from November 4 till November 14. Here you can get more detailed information regarding the affected banks and U.S. Treasury Department restrictions: <http://phishing-911.usbanker.org/bb/41974974/> <http://security.usatreasury.net/255445/> Federal Reserve Bank System Administration".

No envíe nunca datos confidenciales a través de correo electrónico. Existe la creencia de que éste es un método más seguro que utilizar el formulario de compra de la propia página, pero es totalmente falsa. Los delincuentes pueden interceptar esos mensajes.

Utilice su instinto. En muchas ocasiones el aspecto de una página web es un indicio de que nos encontramos frente a un comercio online inseguro. Si tiene dudas, busque referencias positivas en Internet. Si no encuentra ninguna, ni buena ni mala, considere que es como si fueran negativas. A veces los cibercriminales crean páginas que duran muy poco tiempo, tan sólo el necesario para que unos cuantos usuarios desprevenidos sean estafados.

Y finalmente piense que esa idea de "y por qué alguien va a atacarme a mi, un simple usuario de la Red", es precisamente la que tienen en mente los delincuentes de Internet. Y tenga por seguro que están sacando muy buen provecho de ella.

5. Conclusiones: consejos básicos para operar con seguridad en Internet

- **Compruebe las características de seguridad de la página** en la que va a operar (uso de protocolo seguro, sello de certificación de seguridad)
- **Mantenga siempre actualizado el sistema operativo** y las aplicaciones que tenga instaladas en su PC
- **No ejecute nunca archivos que provengan de fuentes sospechosas**
- **Antes de hacer una compra online o de acceder a un servicio bancario de Internet asegúrese de que no existe ningún virus activo en el PC**
- **No pague nunca nada en Internet sin estar totalmente seguro** de la honradez del vendedor
- **Complemente su antivirus tradicional con tecnologías proactivas** que detecten amenazas sin necesidad de actualizaciones
- **Si está pujando por un artículo en una web de subastas, desconfíe de ofertas que puedan llegarle por otro medio** que no sea el del propio portal de subastas
- **Utilice herramientas antivirus de "segunda opinión"** para descartar la presencia de malware en su PC
- **No envíe nunca datos confidenciales a través de correo electrónico**
- **No haga caso nunca a los mensajes de spam publicitarios** ni a aquellos que digan provenir de entidades financieras y soliciten datos confidenciales
- **Utilice su instinto.** Muchas veces el aspecto de una página web es un indicio de que nos encontramos frente a un comercio online inseguro
- **Antes de comprar en un comercio online es muy recomendable investigar sobre la reputación del vendedor**

EN RESUMEN

El aumento de las transacciones online y del tiempo libre hacen de la Navidad uno de los periodos más peligrosos para los usuarios de Internet, ya que los ciber-delincuentes aumentan el número de ataques contra ellos. Por ello, conviene mantenerse alerta y tomar las medidas de seguridad adecuadas. En caso contrario, los usuarios corren el riesgo de que su dinero acabe en las manos de los delincuentes de la Red.

1 <http://www.cecarm.com/servlet/s.SI?METHOD=DETALLENOTICIA&sit=c,731,m,2627&id=20874>

2- <http://www.forrester.com/ER/Press/Release/0,1769,1233,00.html>