



Consejos para una Navidad Segura



INDICE

1. Compras online	2
2. Juegos online	4
3. Mensajería instantánea y correo	5
4. Consejos para disfrutar del pc en navidad de manera segura	6



La Navidad es una de las fechas preferidas por los ciber-delincuentes para aumentar el número de sus ataques. La razón es sencilla: al disponer de más tiempo libre, aumenta el número de personas que se conectan a Internet. Esto hace que también aumenten las posibilidades de que una de ellas se convierta en víctima de sus delitos.

Vamos a repasar cuáles son los principales riesgos de este período vacacional, y la forma en que los usuarios pueden evitarlos.

1. COMPRAS ONLINE

En **Navidad aumenta el número de transacciones online**, debido a la compra de regalos navideños. Por ejemplo, el lunes después de acción de gracias -un día conocido como ciber-lunes por ser el primero de las compras navideñas-, el número de estadounidenses que realizó una compra online aumentó un 38% con respecto al 2006¹.

El año pasado, la cifra de compradores que hicieron sus compras de navidad de manera online en **EEUU alcanzó los 13,5 millones**².

En resumen, en Navidad aumenta el número de dinero que se transfiere de forma online. Los ciber-delincuentes son conscientes de ello y por eso aumentan sus ataques. El riesgo para los consumidores puede venir de varios frentes. El primero de ellos será el **phishing**. Se trata de correos que simulan proceder de una entidad bancaria o servicio de compra online, pero que son falsos. Generalmente, se pide al usuario que pinche sobre un link y proporcione sus claves bancarias. Si el usuario lo hace, estará dando esas claves a los ciber-delincuentes.



El año pasado el número de ataques de phishing lanzados durante el mes de diciembre aumentó un 56% respecto al mismo período del año anterior, superándose la cifra de los **23.000 ataques**³.

1- <http://www.cnnexpansion.com/economia/2007/11/28/eu-logra-record-de-compras-on-line>

2- <http://www.bnd.com/business/story/193659.html>

3- Datos procedentes del Anti-Phishing Working Group.



El de los **troyanos** es el segundo riesgo al que se enfrentan los consumidores online. Muchos de estos códigos maliciosos están diseñados para robar datos bancarios (claves, número de cuenta,...). Son los llamados troyanos bancarios. Estos han supuesto un 18,59%⁴ del total de malware creado en 2007. Su funcionamiento es muy variado, desde capturar las pulsaciones del teclado hasta redireccionar a una página falsa de una entidad bancaria, todo con el fin de hacerse con el dinero de los usuarios. Por eso los compradores online deben estar seguros de que su ordenador se encuentra libre de códigos maliciosos antes de realizar cualquier transacción online.

¿Cómo llegan los troyanos al ordenador?

Este tipo de malware no se distribuye por sí mismo, por lo que necesita la colaboración involuntaria del usuario para ejecutarse. Para ello, se "disfrazan" como archivos que contienen fotos, trailers de películas,..o cualquier otro contenido atractivo, de modo que el usuario se vea tentado a abrirlos. En otras ocasiones, el cebo es un link que dice



llevar a uno de esos contenidos. Si el usuario abre el archivo o pincha sobre el link, estará introduciendo uno de estos códigos maliciosos en su sistema.

Los compradores online deben ser precavidos, ya que se estima que en 2006, el importe medio robado a cada víctima mediante estas técnicas ha sido de 6.383 €⁵.

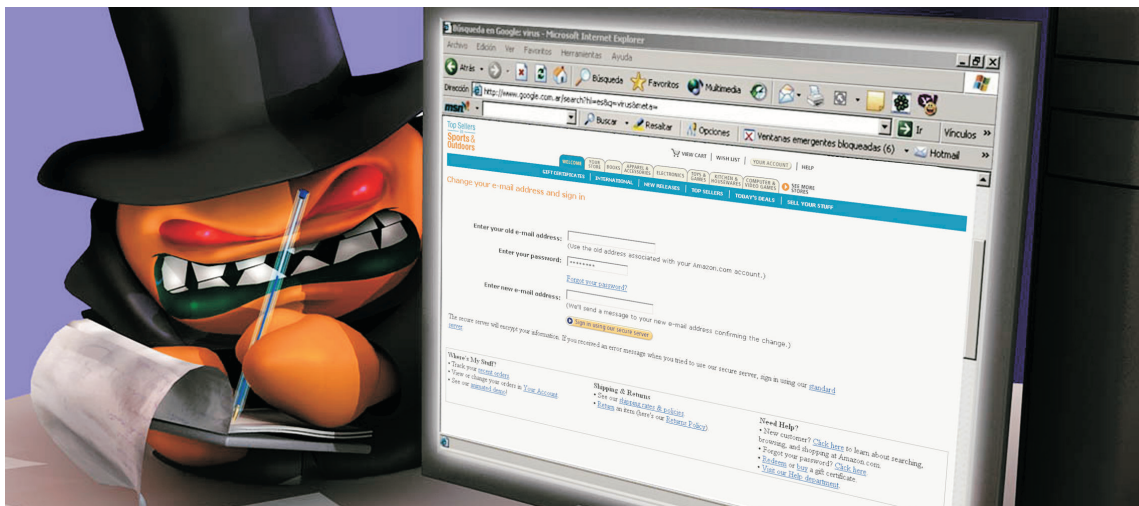
Otro riesgo que amenaza a los compradores online es el de las **falsas web de subastas** o ventas de productos. En muchas se ofertarán productos a precios increíbles, tanto que deberían hacer sospechar a los usuarios. Si se compra en una de esas webs, es probable que no se reciba el producto y que, además, se pierda el dinero pagado. Por eso, conviene investigar un poco sobre la fiabilidad de la página en cuestión antes de realizar ninguna compra.

Un truco muy sencillo para comprobar la fiabilidad de una web es ver si la conexión con ella se produce a través del protocolo SSL. Éste es un protocolo que permite realizar la transferencia de datos entre el PC y el servidor de forma segura y privada, de modo que la información no pueda caer en manos de un tercero. Otro truco rápido y sencillo es teclear el nombre de la página en un buscador y leer algunas opiniones de los consumidores. Si hay muchas quejas sobre productos que no llegan o que son defectuosos, sabremos que no debemos comprar en esa web.

4- Datos procedentes de PandaLabs, el laboratorio de detección y análisis de malware de Panda Security.
5- Datos procedentes del Anti-Phishing Working Group.



2. JUEGOS ONLINE



En Navidad tanto los jóvenes como los mayores disponen de más tiempo libre. Mucho de ese tiempo se gasta en jugar online con otros usuarios remotos. En los últimos meses se ha detectado un gran número de variantes de códigos maliciosos diseñados para robar las claves de estos juegos.

Al robar estas claves, **los ciber-delincuentes persiguen un beneficio económico**, ya que éstas pueden alcanzar un importante valor en el mercado negro de Internet. La razón es que hay muchos objetos, funcionalidades, etc. de esos juegos que se consiguen en función del grado de experiencia. Aquellos que no sean capaces de lograr ese grado, no dudarán en pagar una importante cantidad de dinero por conseguirlos. Esto lo aprovecharán los delincuentes de la red para venderlos al mejor postor a través de foros, páginas de subastas, etc.

Pero los juegos online pueden presentar otros problemas, ya que muchos de ellos permiten crear un perfil de usuario.

En él se publica, a menudo, la dirección de correo electrónico del jugador. La idea es que los usuarios se comuniquen entre sí, compartiendo trucos y experiencias. Sin embargo, los ciber-delincuentes aprovechan esta información para personalizar sus envíos. Así, enviarán correos electrónicos que dirán contener plugins para el juego o imágenes de éste, para incitar a los usuarios de ese juego a abrir el archivo adjunto o seguir un link. Si lo hacen, realmente estarán introduciendo un código malicioso en su sistema.

El envío de archivos que dicen contener el juego, la puesta a disposición del mismo a través de redes P2P, etc., son otros de los medios que emplean los ciber-delincuentes para aprovechar el interés de los usuarios por estos juegos para distribuir sus creaciones.



3. MENSAJERÍA INSTANTÁNEA Y CORREO



El uso de la **mensajería instantánea** como medio de comunicación es hoy casi generalizado. Herramientas como MSN Messenger, Yahoo Messenger, etc. son algunas de las más usadas en los hogares, sobre todo, por los jóvenes. Por ello, se han convertido en uno de los medios más empleados por los ciber-delincuentes para distribuir sus creaciones. Generalmente, envían links o archivos que parecen provenir de uno de nuestros contactos. Sin embargo, se trata de un gusano intentando propagarse a otros usuarios. Si uno de ellos pincha sobre el link o ejecuta el archivo, quedará también infectado.

Una técnica similar se emplea para distribuir el malware a través de **correo electrónico**. En Navidad uno de los métodos más comunes de distribuir estos

códigos maliciosos es la oferta de tarjetas de felicitación gratuitas. Se trata de correos que ofrecen al usuario una divertida tarjeta de felicitación que podrá enviar a sus seres queridos. Para conseguirla deberá pinchar un link o descargar un archivo. En ambos casos, el resultado final será la infección con un ejemplar de malware.

En otras ocasiones, el código malicioso se **"disfrazará"** de trailer de película o de códec necesario para ver la misma, aprovechando el gran número de estrenos cinematográficos que se producen en Navidad. Se trata, de nuevo, de un cebo para incitar al usuario a realizar una acción que le conducirá a estar infectado.



4. CONSEJOS PARA DISFRUTAR DEL PC EN NAVIDAD DE MANERA SEGURA

1. Antes de hacer una compra online o de acceder a un servicio bancario de Internet asegúrese de que no existe ningún malware activo en el PC. Para ello, complemente su antivirus tradicional con tecnologías proactivas que detecten amenazas sin necesidad de actualizaciones y utilice herramientas antivirus de **"segunda opinión"** para descartar la presencia de malware en su PC.
2. **No haga caso nunca a los mensajes de spam** publicitarios ni a aquellos que digan provenir de entidades financieras y soliciten datos confidenciales.
3. **Investigue** sobre la reputación del vendedor antes de comprar en un comercio online.
4. **Mantenga siempre actualizado el sistema operativo y las aplicaciones** que tenga instaladas en su PC. Las vulnerabilidades del sistema pueden ser una puerta de entrada para el malware e, incluso, permitir a un ciber-delincuente tomar el control de su PC.
5. **No ejecute** nunca archivos ni siga links que provengan de **fuentes sospechosas**. Además, si le llega un archivo a través de mensajería instantánea, asegúrese de que se lo ha enviado su contacto y que no es un malware intentando propagarse.
6. No pague nunca nada en Internet sin estar totalmente seguro de la **honorabilidad del vendedor**. Si está pujando por un artículo en una web de subastas, desconfíe de ofertas que puedan llegarle por otro medio que no sea del propio portal de subastas. Podría quedarse sin el producto y sin su dinero.
7. **No envíe nunca datos confidenciales** a través de correo electrónico, mensajería instantánea, chats u otro tipo de canales similares.

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.*



