

Consejos de seguridad para Navidad

Navidad se acerca a paso veloz, y las diversas actividades en línea se incrementan significativamente. Los consumidores están ocupados comprando obsequios y aprovechando las baratas, los comerciantes en Internet se dedican a liquidar su mercadería con descuentos de fin de año, y los sitios de entretenimiento están atestados con deslumbrantes tentaciones. El tráfico en Internet, en consecuencia, se eleva al máximo en esta época del año.

Pero, debido a que todo el mundo está concentrado en divertirse y gastar dinero, se presta (aún) menos atención de lo habitual a los problemas de seguridad. Esto, convierte a la Navidad en un excelente momento para cometer delitos cibernéticos. Sin perder tiempo, los piratas informáticos utilizan este periodo agitado, para aprovecharse de las personas que están pensando en cualquier otro asunto, menos en la seguridad.

En esta edición de **Conociendo más sobre seguridad informática**, ofrecemos algunos consejos de seguridad, para evitar los peligros en línea esta Navidad.

Consejo 1: **Ser cuidadoso con el correo no deseado y la falsificación de sitios**

Hemos comentado en varias oportunidades los [riesgos del correo no deseado](#) y de la [falsificación de sitios](#).

Los piratas agudizan su creatividad y astucia en esta época del año, con el fin de persuadir a sus víctimas y lograr que caigan en la trampa.

Por lo tanto, es fundamental permanecer siempre alerta y ser extremadamente cautelosos al revisar esos mensajes electrónicos con "descuentos especiales".

A continuación describimos los principales riesgos de seguridad, provenientes del correo electrónico no deseado y la falsificación de sitios:

1. Archivos adjuntos infectados

No es extraño recibir un mensaje electrónico, aparentemente enviado por un amigo o colega, con un archivo adjunto peligroso, que incluye un virus u otro programa malicioso.

O, tal como sucede a menudo en la época de las fiestas, es frecuente el envío de tarjetas navideñas, protectores de pantalla o paquetes de "caritas" (*emoticons*), para el divertimento de los usuarios.

Probablemente, el remitente sea desconocido para quienes reciben este tipo de mensajes, pero es Navidad, de modo que no hay por qué preocuparse, ¿verdad?

Grave error: es altamente probable que el archivo adjunto incluya un "obsequio", que nadie querría para Navidad.

☑ Una "carita" o *emoticon* es un símbolo gráfico que se utiliza en las comunicaciones a través del correo electrónico y sirve para expresar el estado de ánimo del remitente.

Aunque, actualmente, la mayoría de las personas se dan cuenta de que no deben abrir archivos adjuntos provenientes de fuentes no conocidas, un mensaje electrónico de un amigo podría inducirnos a ser más confiados de lo habitual.

Pero, detengámonos y pensemos por un momento. El ordenador de ese amigo, ¿no podría estar infectado con un troyano, que envía mensajes de correo electrónico a todas las personas en su lista de contactos?

Al meditar un poco la cuestión, tiene sentido utilizar unos segundos, para analizar cualquier archivo adjunto en busca de virus y programas espía, incluso si pensamos que es de alguien conocido.

El escepticismo saludable nunca le hizo daño a nadie.

2. Descargas automáticas de código malicioso como resultado del aprovechamiento de una vulnerabilidad

Un ordenador puede infectarse con programas espía, virus o troyanos simplemente visitando un sitio de Internet que haya sido vulnerado con código malicioso, ya sea de manera accidental o deliberada.

Los servidores de Internet que, en condiciones normales albergan sitios legítimos, también pueden ser comprometidos y obligados, por delincuentes informáticos, a distribuir código malicioso a los ordenadores de personas desprevenidas.

Estas amenazas podrían incluir decenas de mensajes de correo electrónico no deseado que contienen, aparentemente, algo tan inofensivo como un enlace a un sitio corrupto.

Este vínculo, podría infectar automáticamente un ordenador, que no tenga instalados los últimos parches para el sistema operativo y el navegador.

Por lo tanto, es necesario asegurarse de contar siempre con las **últimas actualizaciones y parches instalados**, cuya descarga es gratuita.

También hay que desconfiar de los enlaces reenviados por alguien desconocido.

Antes de acceder a algún sitio por primera vez, es recomendable utilizar un verificador de direcciones de Internet, y elevar los valores de seguridad de su navegador al nivel **alto** para evitar la ejecución de guiones ActiveX, ya que, a menudo, pueden generar infecciones.

3. Aprovechamiento de vulnerabilidades en el cliente de correo electrónico

Los clientes de correo electrónico pueden contener vulnerabilidades, que permiten que agresores remotos se infiltren en los ordenadores.

Las secuencias de comandos embebidas, o los gráficos con virus pueden enviarse en masa. Este tipo de ataque podría ser muy dañino, si no se contrarresta adecuadamente.

Para evitar que sucedan, es necesario mantener a la aplicación cliente de correo electrónico actualizada con los últimos parches.

Si ésta forma parte del sistema operativo (como por ejemplo, Outlook Express) debemos utilizar el sitio de actualizaciones de Windows.

En el caso de Outlook, hay que dirigirse al sitio de descarga de actualizaciones de Office.

Los usuarios que utilicen un cliente independiente, como Opera o Thunderbird, tendrían que consultar el sitio de Internet del proveedor, para obtener más información acerca de cómo mantener su correo electrónico seguro y actualizado.

4. Mensajes de correo electrónico falsos en busca de información personal

La falsificación de sitios es una tendencia peligrosa que debería controlarse siempre. Básicamente, evitar este tipo de ataques, es cuestión de astucia.

Nunca debemos responder a pedidos comerciales que soliciten datos confidenciales, como por ejemplo, información de ingreso al sistema, verificación de tarjetas de crédito, detalles de membresía y otras artimañas evidentes.

Las organizaciones serias nunca realizarían pedidos de esa naturaleza por correo electrónico.

Consejo 2: Ser cuidadoso con las operaciones en línea

1. Datos cifrados y certificados de seguridad

Generalmente, al efectuar el pago de un artículo o servicio a través de Internet, la información enviada se cifra en el ordenador que realiza la operación, y se descodifica cuando llega al receptor, para que sea incomprensible mientras está en tránsito.

De esta forma, los piratas que traten de interceptar los detalles de la sesión de la operación, manipulando el canal de conexión, solamente verán símbolos ilegibles que no podrán ser utilizados.

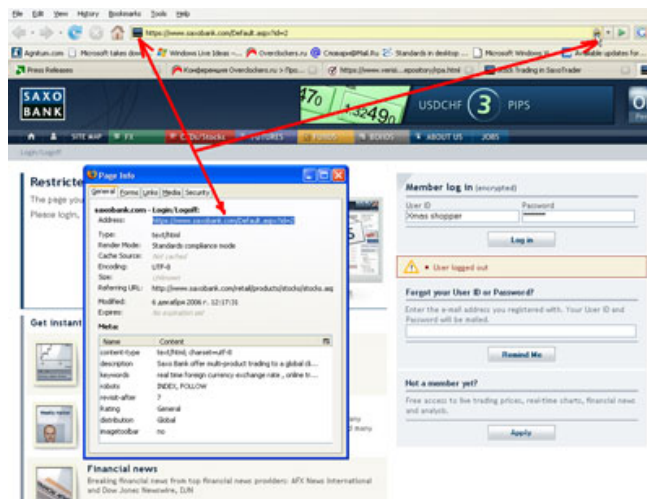
Los navegadores modernos pueden cifrar datos confidenciales rápidamente, al enviarlos hacia Internet.

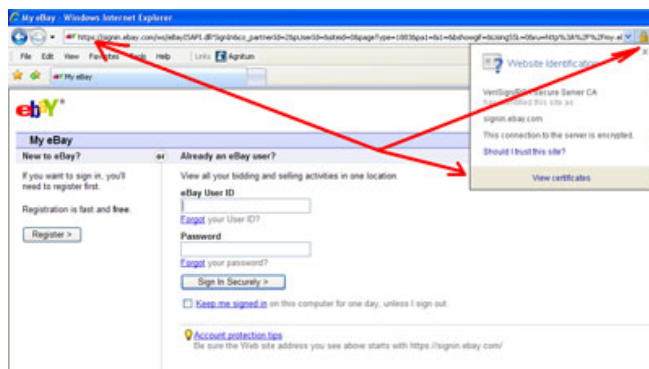
Se debe tener en cuenta que, al realizar compras en distintos sitios de Internet, la información confidencial ingresada siempre debe transmitirse en formato cifrado.

Siempre hay que buscar el icono del candado amarillo a la derecha de la barra de direcciones.

Este icono y el prefijo **https** en el recuadro con la dirección, son indicadores de que el sitio es seguro.

Se puede pulsar sobre él, para ver información adicional acerca del certificado de seguridad y la autenticidad del sitio.





2. Establecer relaciones únicamente con organizaciones creíbles

Naturalmente, todos deseamos tratar con entidades de confianza, cuando nuestra información financiera personal está en juego. Lo ideal es verificar siempre los sitios de comercio electrónico desconocidos, antes de brindar cualquier información personal clave.

Se puede investigar la reputación del sitio, realizando una simple búsqueda en Google. Además, es importante verificar las propiedades de registro del sitio (<http://www.networksolutions.com/whois/index.jsp>), e investigar en profundidad los certificados de seguridad y las autoridades emisoras.

3. Utilizar las tarjetas de crédito con inteligencia

Al realizar operaciones financieras en Internet, debemos asegurarnos de verificar, en forma regular, los registros de nuestras tarjetas de crédito, e informar inmediatamente cualquier discrepancia a la organización responsable. Por supuesto, es fundamental no divulgar nunca los detalles de la tarjeta de crédito, a alguien que no sea de confianza. También resulta conveniente, crear una política de comunicación hogareña, que establezca reglas para determinar el nivel de información de las tarjetas, que pueden utilizar los niños. Outpost Firewall Pro permite definir una lista de caracteres (como por ejemplo, el número de la tarjeta) para que este sea bloqueado y no se transmita a través de Internet, evitando así la divulgación accidental.

Consejo 3: Utilizar el sentido común

1. Nunca abrir archivos descargados de Internet, sin verificarlos primero en busca de virus y programas espía.
2. Instalar un cortafuegos que proteja el ordenador contra los ataques de red y contra programas ilegítimos.
3. Las redes con conexión punto a punto, pueden estar llenas de código malicioso, por lo tanto, debemos ser cuidadosos al intercambiar archivos multimedia.

Además, es útil recordar que en este tipo de redes, podría circular muchísimo material con derechos de autor.

Los virus que se propagan a través de los mensajeros instantáneos, se están haciendo cada vez más comunes. Por lo tanto, es conveniente tener cuidado al intercambiar enlaces y archivos a través de este medio de comunicación, incluso con amigos.

Mantener siempre los programas actualizados, especialmente aquellos que acceden a Internet. Para mayor información más acerca de este tema, consulte [La actualización de programas como medida de seguridad](#).

Y un último deseo por hoy:

¡Tengan todos una muy feliz Navidad y próspero año nuevo!