

Recomendaciones de Seguridad en Internet

Cualquier usuario que tenga un equipo que esté conectado a una red debe tener en cuenta unas consideraciones de seguridad que resumimos a continuación.

Si tenemos el PC con Windows conectado a una red, lo más probable es que tengamos configurada la red para Trabajo en Grupo de Microsoft. Esto nos permite intercambiar información entre los distintos ordenadores que integran la red, de manera que podamos compartir recursos (directorios, impresoras, etc...) para que el resto de los equipos tengan acceso a ellos. Si esto es así, deberemos tener en cuenta algunas medidas de seguridad:

1. Elimine del PC los protocolos de red que no sean necesarios para conectarse a Internet. Es decir, todos excepto el protocolo TCP/IP. Esto se realiza desde Inicio -> Panel de Control -> Red, seleccionando el protocolo a eliminar y pulsando Quitar.
2. No comparta archivos o impresoras a través del protocolo TCP/IP. Para ello desde Inicio -> Panel de Control -> Red, elija el protocolo TCP/IP y pulse en Propiedades. Luego seleccione la pestaña Enlaces y desmarque Compartir Impresoras y Archivos para Redes Microsoft.
3. Deshabilite NetBIOS sobre TCP/IP para evitar que el intruso pueda ver los recursos que esté compartiendo en el PC. Para deshabilitarlo volvemos a elegir el protocolo TCP/IP, pulsamos Propiedades y seleccionamos la pestaña NetBIOS, ahí se desmarca la opción NetBIOS. Si no se permite desmarcarlo es que ya está deshabilitado.
4. No comparta recursos si no es necesario. Si necesita compartirlos, hágalo siempre con una buena contraseña y asegúrese de que el recurso se comparte con las personas que lo necesitan y no esté accesible para todo el mundo.
5. Siempre que sea posible, compártalos como de "sólo lectura". Así evitará que, accidentalmente o malintencionadamente, le borren información o le saturen el disco duro escribiendo en el directorio compartido.
6. NUNCA comparta su disco duro con privilegios de escritura ni siquiera con contraseña. Hay programas que realizan diversos tipos de ataque (de fuerza bruta, diccionario, etc..) hasta que dan con la contraseña correcta. Un hacker tiene todo el tiempo del mundo para probar, y Windows no le avisa de que lo está haciendo.
7. NUNCA facilite sus claves personales a través del correo, chat o Messenger. Los delincuentes aprovechan las últimas tecnologías para hacerse con las claves personales de internautas poco precavidos.
8. Apague el PC cuando no use la conexión. Es más seguro y ahorrará energía.

En general, le recomendamos que no comparta información importante de forma permanente por este método, pues no proporciona demasiada seguridad.

Los virus, troyanos y spyware pueden camuflarse dentro de otro tipo de programas. Por este motivo es muy importante tener la absoluta seguridad de que el software que descargamos de Internet proviene de una fuente fiable.

Los virus informáticos son programas que se propagan ocultos dentro de otro programa, correo electrónico, página web, o fichero. Los virus alteran el correcto funcionamiento del PC. Entre otras cosas, pueden llegar a eliminar información del disco duro, o hacer que el ordenador se reinicie cada pocos minutos, o incluso abrir puertos de comunicaciones permitiendo que un intruso controle el ordenador de forma remota.

El software proveniente de un sitio poco fiable tiene más posibilidades de contener virus, troyanos o spyware camuflado.

Es muy recomendable analizar todos los programas descargados de Internet con el programa antivirus y desconfiar de las descargas realizadas desde sitios "alternativos" (P2P, etc) o que ofrezcan poca seguridad.

Ante la duda, lo más conveniente es descargar los programas directamente desde la web del fabricante.

Desconecte el módem telefónico. Si navega con el cablemódem de PTD no le afectarán los dialers.

Los dialers se utilizan para redirigir de forma maliciosa las conexiones mientras se navega por Internet. Su objetivo es colgar la conexión telefónica que se está utilizando en ese momento y establecer otra, marcando otro número. Se puede llegar a recibir una factura telefónica de importe desorbitado. Los dialers solamente pueden causar problemas en accesos de banda estrecha (por módem telefónico) ya que los accesos de banda ancha no requieren marcar ningún número de teléfono. Para desconectar el ordenador de la línea telefónica básica sólo es necesario desconectar el cable telefónico del antiguo módem.

Mantenga actualizado su Sistema Operativo. Cada cierto tiempo aparecen vulnerabilidades en los sistemas operativos más utilizados. Estas vulnerabilidades son aprovechadas por los hackers para acceder a su ordenador con los más diversos fines.

Instale y mantenga actualizado un antivirus.

El número de virus informáticos que amenazan la integridad de su equipo crece día a día. Por este motivo es importante no sólo mantener instalado y activo un antivirus, sino actualizado.

Utilice un programa anti-Spyware.

Un programa Adware es aquel que presenta anuncios al usuario mientras está siendo utilizado. Estos anuncios, aunque molestos, soportan parte del coste de desarrollo del programa. Muchas veces, este tipo de programas adware transmiten datos de navegación, o incluso datos personales, como las pulsaciones del teclado del usuario, sin su consentimiento. A estos programas se les denomina Spyware (Programas espía).

Además del perjuicio que supone para la intimidad, los programas Adware y Spyware tienen otro efecto en el ordenador. Aunque no se muestren claramente, estos programas permanecen residentes en memoria y ralentizan el funcionamiento del PC.

Utilice un firewall correctamente configurado.

Un firewall es un "cortafuegos" entre su ordenador e Internet. Esto evita que un usuario malintencionado, un programa espía o cualquier otra amenaza accedan a su ordenador a través de los puertos más vulnerables de su sistema operativo.

Esos puertos son utilizados por diversos programas diseñados para tomar control de su ordenador, espiar sus actividades online o borrar su disco duro.

En los últimos tiempos se ha puesto de moda un delito muy extendido, el phishing, a través del cual los delincuentes se hacen pasar por una entidad bancaria que solicita las claves de acceso a la cuenta del usuario. Por seguridad, los bancos NUNCA solicitan datos directamente a través de medios electrónicos a sus clientes, sino que es necesario acercarse personalmente hasta la sucursal.

Si tiene hijos pequeños, controle los lugares a los que acceden. No todos los contenidos que se pueden encontrar en Internet son apropiados para los más pequeños. Muchas veces, los niños pueden visualizar contenidos sexuales o violentos por azar, sin el control de los padres. El control de la navegación que realizan los más pequeños es imprescindible para que Internet sea una herramienta útil y segura para ellos. El mercado ofrece numerosas soluciones para asegurar una navegación segura de los niños.

No propague las cadenas de mensajes.

Las cadenas de mensajes se han convertido en una de las mayores lacras de Internet. Cada día aparecen cientos de cadenas solicitando reenviar un mensaje de correo electrónico a toda la lista de contactos de un usuario.

A estas cadenas se las conoce con el nombre de Hoax, y sólo tienen como objetivo la recopilación de mensajes de correo electrónico con fines comerciales y la saturación de las redes por el envío masivo de este tipo de correos.

Todas las historias aparecidas en este tipo de cartas pertenecen a la categoría de leyendas urbanas, y lo mejor que se puede hacer con ellas es eliminarlas de la bandeja de entrada sin reenviarlas.

Romper las cadenas de mensajes no sólo no trae siete años de mala suerte, sino que garantiza siete años de tranquilidad en el buzón de correo.

No abra los correos electrónicos no solicitados ni de remitentes desconocidos. Incluso si conoce al remitente, tenga la máxima precaución ante los archivos adjuntos, sobre todo si son ejecutables. Ante la duda, confirme el envío.

La mayor parte de los virus se propagan a través del correo electrónico. Si recibe un mensaje sospechoso, de remitente desconocido o con archivos adjuntos ejecutables, no lo abra, puede contener un virus.

Incluso si conoce al remitente, tenga la máxima precaución antes de abrir los archivos adjuntos, sobre todo si son ejecutables. Ante la menor duda, confirme el envío con el remitente y asegúrese del contenido del correo.

Si sospecha que un correo puede contener un virus, elimínelo sin leerlo y vacíe la papelera de reciclaje de su programa de correo. Ante los mensajes sospechosos, siempre es mejor prevenir que arreglar los desperfectos causados por un virus.

Recuerde que siempre debe mantener un programa antivirus activado y actualizado. Los programas antivirus más avanzados escanean el correo entrante en tiempo real para prevenir la descarga de archivos infectados.

Aún así, ante la duda siempre es preferible borrar el mensaje sospechoso.

Correo electrónico no solicitado (SPAM)

Son e-mails no solicitados, que normalmente buscan de vender algo y provoca una pérdida de tiempo para el usuario ya que tiene que molestarse en identificarlos y borrarlos para que no le ocupen espacio en su buzón.

Si publica notas en alguna web o grupo de noticias, utilice una cuenta de correo alternativa. De la misma forma que no da su número de teléfono a extraños, tampoco lo haga con su correo electrónico. Siempre que en una web le soliciten un registro, lea despacio las condiciones y asegúrese de lo que harán con esa información.

Si recibe muchos e-mails no deseados del mismo remitente, bloquéelo con los filtros de su programa de correo, para hacer que esos mensajes sean rechazados o enviados directamente a la papelera.

Nunca responda a un spam. Es una señal inequívoca de que su cuenta está activa. Igualmente, no visite una página o pulse sobre una imagen que aparezca en un correo de este tipo.

Si no quiere recibir spam, cuando envíe un mensaje a las news (o foros) escriba algún identificador que haga imposible que pueda ser recogido de forma automática por programas informáticos (nombre@QUITAESTOdominio.com, nombre@dominioESTONOVALE.com), tanto en la dirección de correo de la cabecera del mensaje como en la firma. Hágalo siempre a la derecha de la arroba y nunca en el nombre.

Seguridad en
6/5
¿

Para cualquier cuestión le atenderemos en soporte@pastorini.es.