

Seguridad básica en Internet

Autor emanuel martinez
domingo, 06 de julio de 2008
Modificado el martes, 15 de julio de 2008

Seguridad básica en Internet

La seguridad se basa en la probabilidad. Nada es completamente seguro, ni existen programas invulnerables, pero cuando más precavido seas, existen menos probabilidades de que violen tu seguridad. Esto es lo que suele ocurrir en las viviendas: si vives en un primero sin rejas es más fácil que te roben que si vives en un séptimo con ellas (aunque no sea 100% seguro).

Por supuesto, existen auténticos obsesos de la seguridad, que piensan que la CIA puede registrar su ordenador en cualquier momento y sobreprotege todos sus ficheros y operaciones. En el lado opuesto está la mayoría de los usuarios que desconoce o no aplica ciertas normas básicas de seguridad que podrían evitar muchos de estos "agujeros de seguridad".

En este artículo se describe un manual de seguridad mínima.

Firewall

Es un programa que intercepta todas las entradas y salidas de comunicaciones (intranet, internet, etc...) y mediante una serie de reglas permite o prohíbe ciertas acciones. Por ejemplo, si un programa nuevo intenta acceder a Internet pide confirmación al usuario. Este caso se da muy a menudo con programas de tipo Spyware que recopilan datos del usuario y los envían a su creador con fines malintencionados.

Existen firewalls gratuitos, entre los que destacan ZoneAlarm (para principiantes) y Kerio (para usuarios más expertos).

Almacenamiento electrónico de datos confidenciales

Muchos usuarios no tienen conocimiento de lo que puede implicar que alguien descubra ciertos datos confidenciales, y por eso se relajan a la hora de guardarlos: no son pocos los usuarios que guardan en un fichero de texto sus datos bancarios, incluida la contraseña.

Es recomendable guardar los datos confidenciales en un fichero encriptado (o programa de utilidad en su defecto), de modo que solo la persona interesada pueda acceder a dichos datos. El programa PGP es gratuito y permite encriptar fácilmente y con un alto nivel de seguridad cualquier fichero.

Política de contraseñas

Las contraseñas deben ser algo difícil de averiguar y por eso no debemos facilitarles el trabajo a quienes quieran conocerla ilícitamente.

Muchos usuarios utilizan su DNI o su fecha de nacimiento para acceder a todos los webs. Piensan: "así no se me olvida".

Esto puede tener un desagradable desenlace ya que son datos fáciles de conseguir.

Es recomendable usar todo el tamaño del campo permitido para las contraseñas, con mayúsculas y minúsculas intercaladas, y con números si se permiten. Además, las contraseñas deben ser distintas en los distintos sitios en los que el usuario las use.

Algunos métodos usados para averiguar contraseñas usan diccionarios de palabras, por lo que es recomendable usar palabras sin sentido o que no sean de uso común.

Para la gestión de contraseñas existen muchos programas que te permiten rellenar los datos con comodidad y seguridad. Un ejemplo es el programa gratuito KeyWallet.

Email

Son muchos y variados los problemas de seguridad que vienen derivados del uso del mail. Destacan los siguientes:

-

Spam: El spam es una de las peores plagas en internet: no se debe dar la cuenta de correo en cualquier sitio web o foro. Existen programas que se dedican a recopilar direcciones de email en páginas de internet para enviar spam o vender la lista que han conseguido. Por eso es recomendable usar el método de cuentas desechables (Yahoo! lo llama AddressGuard), de modo que cuando una cuenta nos la estén saturando con spam, la borremos y creamos otra, todo esto conservando la cuenta de email principal. La dirección de email principal debes darla solo a las personas de confianza.

-

Páginas fake: a menudo aparecen estafas por mail que consisten en enmascarar la apariencia de un banco, correo web, etc.. donde tenemos que validarnos. Los estafadores guardan los datos conseguidos en una base de datos y los usan posteriormente para llevar a cabo el timo. Cuidado con esto, no te fies cuando te pidan una contraseña por mail (tampoco por teléfono, claro). Primero verifica la veracidad del remitente y comprueba que estás usando protocolo seguro (https).

Spyware y virus

Los programas Spyware se instalan en tu ordenador sin permiso del usuario con distintos fines: dar páginas vistas a una dirección, recopilar datos del usuario, controlar los hábitos del usuario, etc...

Para limpiar tu ordenador de este tipo de programas se puede usar el programa gratuito Ad-aware.

Los virus son más conocidos por el usuario, por lo que actualmente solo aparecen virus que utilizan vulnerabilidades del sistema operativo o del propio navegador. Para evitarlos se debe instalar un buen antivirus y actualizarlo periódicamente.

Programas P2P

Los programas p2p (peer to peer) son aquellos que permiten compartir ficheros con una comunidad virtual. Son muy conocidos el Kazaa, Emule, Morpheus, etc... Hay que tener cuidado con este tipo de prácticas e informarse bien antes de usarlos dado que muchos tienen en su programación técnicas de Spyware.

Programas de mensajería instantánea

Los programas de mensajería instantánea (MSN Messenger, Yahoo Messenger, etc...) dan la opción de agregar contactos para chatear. Algunos explotan esta opción para hacerse pasar por otras personas o usar distintas vulnerabilidades.

No se deben agregar contactos desconocidos a la libreta de direcciones. Además, yo recomiendo usar programas multiplataforma de mensajería instantánea, a los que no afectan las vulnerabilidades de los grandes programas, y además permiten unificar tus usuarios de distintas plataformas. Un ejemplo de programas de mensajería instantánea multiplataforma es Trillian.

Navegadores

El navegador más usado es el Internet Explorer, pero curiosamente es uno de los que más vulnerabilidades tiene y menos funcionalidades.

Yo recomiendo utilizar navegadores libres, como Firefox o Mozilla, que tienen muchas más funcionalidades y se descubren muchos menos problemas de seguridad.

Autor: Juan Manuel Domínguez

http://alzado.org/articulo.php?id_art=375

Usuarios que han visto este tema también han visto...

- Cómo diseñar páginas Web limpias
- Mejorar ancho de banda del XP Professional
- Mis errores favoritos
- Cómo lograr que nuestros usuarios se registren
- Mi primer empleo