Seguridad en la Red

Conexiones seguras

Seguir unas sencillas reglas evita que nadie tome el control de nuestro ordenador

Una actitud responsable frente al ordenador debe situarse a medio camino entre la paranoia y la despreocupación absoluta. No se trata de ver un peligro tras cada archivo, pero tampoco de actuar como si en Internet nada pudiera pasarnos. La cantidad y calidad de las informaciones que se confían al abrigo de los discos duros y se envían por la Red (nombres de usuario, contraseñas, números de tarjetas de crédito, datos personales, fotografías íntimas…) obliga a dedicar un tiempo a garantizar su inviolabilidad. A fin de cuentas, estas precauciones no son más que el equivalente electrónico a cerrar la puerta con llave al salir de casa.

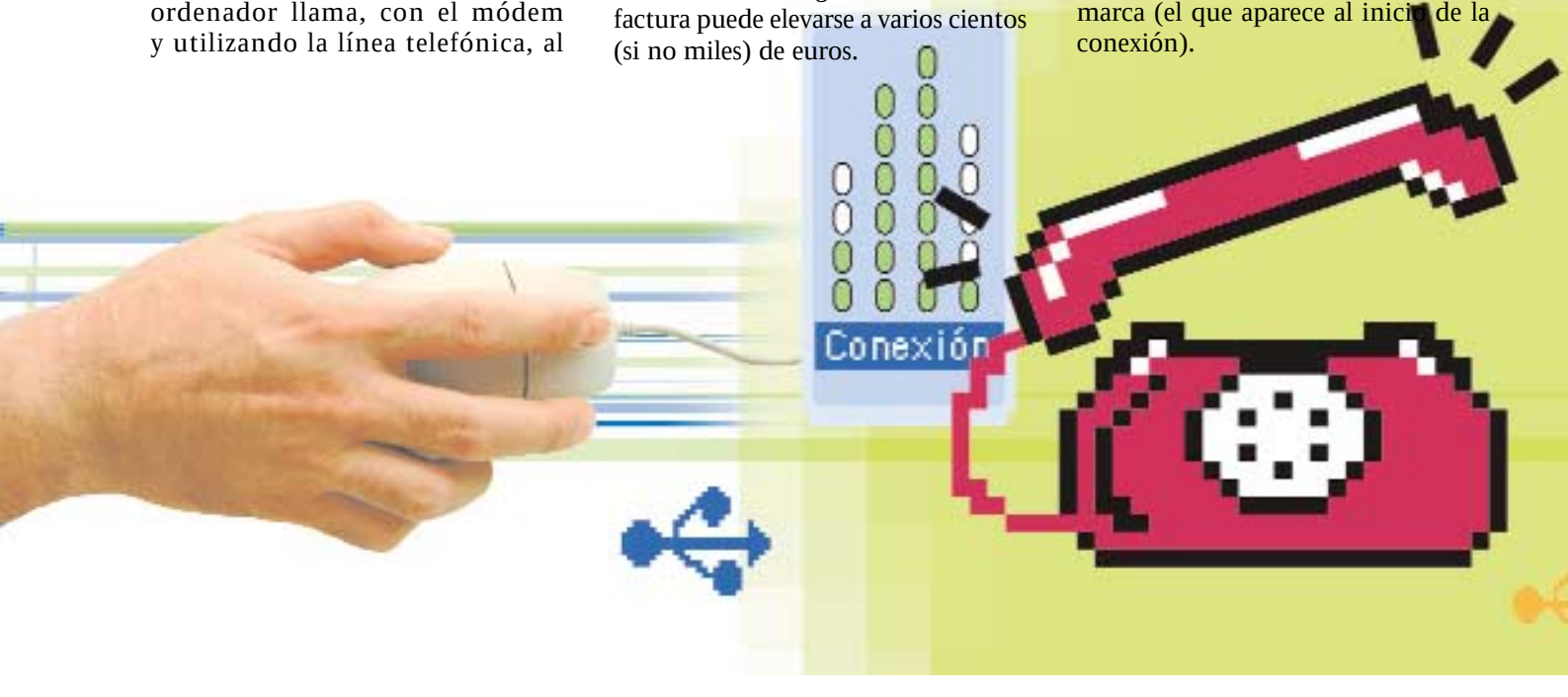
Uno de los timos más habituales en Internet consiste en cambiar subrepticiamente el número de teléfono al que el internauta se conecta. El 87% de los usuarios domésticos españoles entran a la Red por medio de la red telefónica básica (RTB), esto es, su ordenador llama, con el módem y utilizando la línea telefónica, al proveedor de acceso. Por tanto, el internauta paga por dos conceptos: el acceso a Internet (que muchas empresas ofrecen de forma gratuita) y la propia llamada. Lo habitual es que el proveedor de acceso y el usuario se encuentren físicamente cerca para que el coste sea sólo el de una comunicación metropolitana.

Cada vez que el usuario hace doble clic sobre el icono de conexión empieza el proceso: el ordenador llama al número de teléfono seleccionado, se identifica y una vez completada la validación empieza el intercambio de información. Al menos, así debería ser en condiciones normales.

Si un programa malicioso cambia el número de conexión por otro que empiece por 906 será difícil que el usuario lo descubra, ya que no se distingue síntoma alguno: la conexión se abrirá igual, navegará sin ningún problema y la velocidad no se verá alterada. Sin embargo, a fin de mes la factura puede elevarse a varios cientos (si no miles) de euros.

Gasto desorbitado. Pero, ¿por qué iba a querer nadie activar una aplicación que cambia el número de conexión normal por otro tan oneroso para el usuario? Es evidente que no lo hacen por gusto, sino engañados. En ciertas páginas de Internet, generalmente pornográficas, se invita a descargar supuestos programas de chat imprescindibles para acceder a secciones “privadas”. Internautas incautos los descargan y activan y sólo al ver la factura se percatan de su verdadera función: redirigir los parámetros de conexión a sus propios servidores, siempre de tarificaciones abusivas.

Evitar este problema es sencillo: basta con optar por la duda metódica antes de instalar nada: ¿es fiable la fuente de este programa? ¿realmente resulta necesario su uso? Pero, por mucha precaución que uno ponga en práctica, conviene conocer cuál es el número del proveedor de acceso y corroborar cada cierto tiempo que se corresponde con el que realmente se marca (el que aparece al inicio de la conexión).



NAVEGAR A LA CARTA

Enlaces de seguridad
http://webs.ono.com/usr016/Agika

A pesar de su título, no se trata de una mera recolección de enlaces a otros sitios web. “Enlaces de seguridad” es una completa página de consejos útiles detallados de forma coloquial, amena y comprensible. Su apariencia es anticuada, pero incluye información actualizada de las últimas amenazas.

Zone Alarm www.zonelabs.com

Cortafuegos efectivo y fácil de utilizar por los internautas noveles, sin dejar de ser altamente configurable para los más mañosos. Su uso es gratuito para usuarios domésticos.

Tira Ecol http://tira.escomposlinux.org

Los problemas con el ordenador se deben tomar con humor si no se quiere acabar atacado por los nervios. El cómic semanal de Ecol satiriza los quebraderos de cabeza que sufren los que trastean con ordenadores y muestra la cara más amable de tanto cable y sigla ininteligible.

Hay programas que conectan fraudulentamente nuestro PC a un teléfono 906

A buen recaudo

Por muchas precauciones que adopte un usuario, nunca estará completamente a salvo: unas goteras en el techo, un pequeño incendio, un virus especialmente virulento o un amigo poco habilidoso al teclado... son muchos los imprevistos capaces de eliminar el contenido de un disco duro y arruinar el trabajo de meses o años. Por eso, deviene imprescindible que toda la información digital se almacene siempre por duplicado.

Aunque hay sistemas profesionales que simplifican la salvaguarda de datos de forma automatizada y veloz, el dispositivo idóneo para realizar copias de seguridad domésticas es el CD-ROM grabable: es asequible (hay grabadoras por 100 euros y discos compactos vírgenes por 30 céntimos de euro), tiene gran capacidad (650 megabytes, unos 450 disquetes convencionales) y su uso no es complicado.

Si se adopta la precaución de guardar en una carpeta todos los documentos y de traspasarlos periódicamente a un CD (lo que técnicamente se conoce como backup), el usuario siempre contará con un salvavidas al que asirse en caso de catástrofe digital.

Acceso total. En gran medida, el problema viene de que las diferentes versiones domésticas de Windows ofrecen a cualquier programa el control absoluto de la máquina. Esto es, si una aplicación está concebida para borrar todo el contenido del disco duro o para infectar con un virus electrónico a todo lo que se mueva, no habrá nada que lo detenga. Esto no ocurre en Linux, por ejemplo, donde sólo se toma el control total del ordenador en situaciones imprescindibles (cambios de configuración y demás), mientras que el resto del tiempo sólo es accesible la parte menos comprometida del sistema.

Ante este panorama conviene poner un *firewall* o cortafuegos. La labor de esta clase de aplicaciones es la de un matón de discoteca con criterio: cierra las puertas innecesarias y vigila toda la información que entra y sale del ordenador para rastrear si hay algún programa oculto realizando actividades ilegítimas a la espalda del usuario. La susceptibilidad del cortafuegos se puede elevar para que avise de las más nimias amenazas, aunque no conviene situar el listón alto si no se quiere acabar inundado de falsas alertas.

Un cortafuegos mal configurado pierde toda utilidad, ya que se parece a esas alarmas de coche que saltan con el aleteo de una mariposa y despiertan a todo el barrio. Ante la duda, mejor dejar las opciones por defecto para usuarios noveles.