

La seguridad y privacidad del usuario de redes.

Introducción

Navegar por Internet o enviar correos electrónicos puede proporcionar una falsa sensación de seguridad y anonimato.

Sin embargo, nunca debería lanzarse al ciberespacio sin ser consciente de que las páginas que lee, las fotos que ve, los programas que descarga, los correos que envía y recibe dejan un rastro que conduce hasta usted.

La dirección IP de su Pc (el número que le identifica cuando se conecta a Internet); las cookies que acepta de sitios web visitados; su dirección de correo electrónico, que incluye a menudo su nombre completo, constituyen retazos de información que permiten compilar interesantes perfiles acerca de los internautas.

Si además revela confiadamente información personal al rellenar formularios web para suscribirse a servicios gratuitos o participar en sorteos, el rastro que va dejando será fácilmente vinculable a una persona con nombres y apellidos. Y adiós al anonimato.

Los grandes portales de contenidos presentan una amplia oferta de servicios gratuitos: acceso a Internet, correo, página personal, noticias, mensajes a móviles... ¿Gratuitos? El precio que paga es su privacidad.

Estos regalos añadidos buscan financiación alternativa a través de publicidad y del comercio electrónico.

En consecuencia, en los contratos que firma el cliente para suscribirlos, y que raramente lee, se le informa de que encontrará publicidad ajena durante la prestación de los mismos.

Más aún, se le advierte de que tanto la información facilitada durante su registro, como la recopilada a partir del uso que haga del servicio (hábitos, gustos, etc.), podrá ser explotada comercialmente e incluso compartida con terceros, aunque sin desvelar la identidad individual del cliente.

Aún aceptando que las compañías que ofrecen esos servicios no utilicen sus datos más allá del fin con que los recaban, es decir, marketing personalizado para cobrar más a sus anunciantes, ¿quién garantiza que no serán usados por empleados desleales?

El navegante posee hoy valor intrínseco como receptor de publicidad. Cuanto mejor se le conozca, más se cobrará al anunciante.

En una sociedad como la nuestra, muchos usuarios cobrarán gustosos porque se sepa todo sobre ellos.

Otros, en cambio, preferimos salvaguardar nuestra pequeña parcela privada, incluso en Internet.

Extraído del artículo de Gonzalo Álvarez Marañón, Ingeniero en Telecomunicaciones del CSIC (España).

La Protección de Datos personales en Argentina

En octubre del 2000 el Senado argentino dió un importante paso adelante para la protección del derecho a la intimidad de sus ciudadanos, al aprobar una ley que tendrá como fin garantizar a los ciudadanos el control y el libre acceso a la información que de estos posean organismos públicos y privados.

Tras un largo periplo que data de la reforma constitucional realizada en 1994, en la cual se establecía en su artículo 43 el derecho de cualquier ciudadano a preservar su intimidad, y tras enfrentarse incluso a un veto presidencial en 1996, el pasado día 4 del presente mes fue aprobada la ley denominada "Hábeas Data".

Esta ley se encargará de proteger los datos de los ciudadanos argentinos. La citada ley distingue dos tipos de datos, los comunes (nombre, apellidos, dirección, etc.) y los sensibles.

Se consideran como datos sensibles cualquier información del individuo que pueda motivar algún tipo de discriminación por parte de terceros.

Entre estos últimos estarían la raza y la orientación política o sexual. La nueva ley obliga a las empresas a comunicar por escrito a los ciudadanos la inclusión de sus datos personales en sus bases de datos.

De igual forma se establece la obligatoriedad de suprimir o sustituir los datos inexactos de cualquier ciudadano.

Los datos de los ciudadanos deberán ser fácilmente accesibles por los mismos, para ello se establece un plazo de 10 días para responder a la consulta de información de cualquier individuo que previamente haya demostrado su identidad.

Para controlar la aplicación de esta ley se crea un nuevo organismo de control estatal cuya misión será la de vigilar a los organismos públicos y empresas privadas. Este órgano podrá aplicar multas que van desde los 5.000 hasta los 100.000 pesos a quien o quienes ofrezcan información sin consentimiento o errónea. Incluso, se podrá llegar a condenas de 3 años de prisión si se incluyen datos falsos a sabiendas.

Navegación segura en Internet

De todos los servicios que ofrece Internet, como correo electrónico, grupos de noticias, canales de charla, transferencia de ficheros, conexión remota a otras computadoras, etc., sin duda alguna el que mayor crecimiento ha experimentado y mayor popularidad ha cobrado entre los usuarios ha sido la World Wide Web.

Paralelamente y siguiendo los requerimientos del mercado, el software de navegación ha ido evolucionando a un ritmo espectacular, incorporando con cada nueva versión nuevas utilidades y posibilidades en una carrera en la que cada navegador intenta dejar atrás a sus competidores.

El resultado es que los navegadores consumen cada vez más recursos y han terminado por transformarse en herramientas muy voluminosas, con tantos detalles de funcionamiento que resulta difícil seguir la pista de los nuevos servicios añadidos. En su interior se ocultan opciones de configuración de nombres a menudo crípticos y no pocas veces de oscura finalidad.

Por lo tanto, teniendo presente que la mayor parte del tiempo que un usuario va a emplear conectado a Internet será haciendo uso del navegador, es importante conocer todos los detalles de cómo configurar de manera segura la gran cantidad de características que incorporan las últimas versiones.

1)- Obtener un navegador seguro

Puede parecer trivial a primera vista, pero si se reflexiona un poco se comprenderá la necesidad de obtener una **copia válida y segura del navegador** preferido. No hay que olvidar que el navegador goza de acceso ilimitado a los recursos del sistema informático: memoria, disco, conexiones de red, tarjeta de sonido, impresora, vídeo, etc. En otras palabras, si el navegador decidiera comportarse maliciosamente, podría abrir conexiones con máquinas remotas y filtrar información del disco duro hasta infectarlo con otros virus o destruir ficheros valiosos.

Cualquier programa con un potencial dañino semejante no debería nunca considerarse a la ligera.

Configuración segura de Netscape Communicator

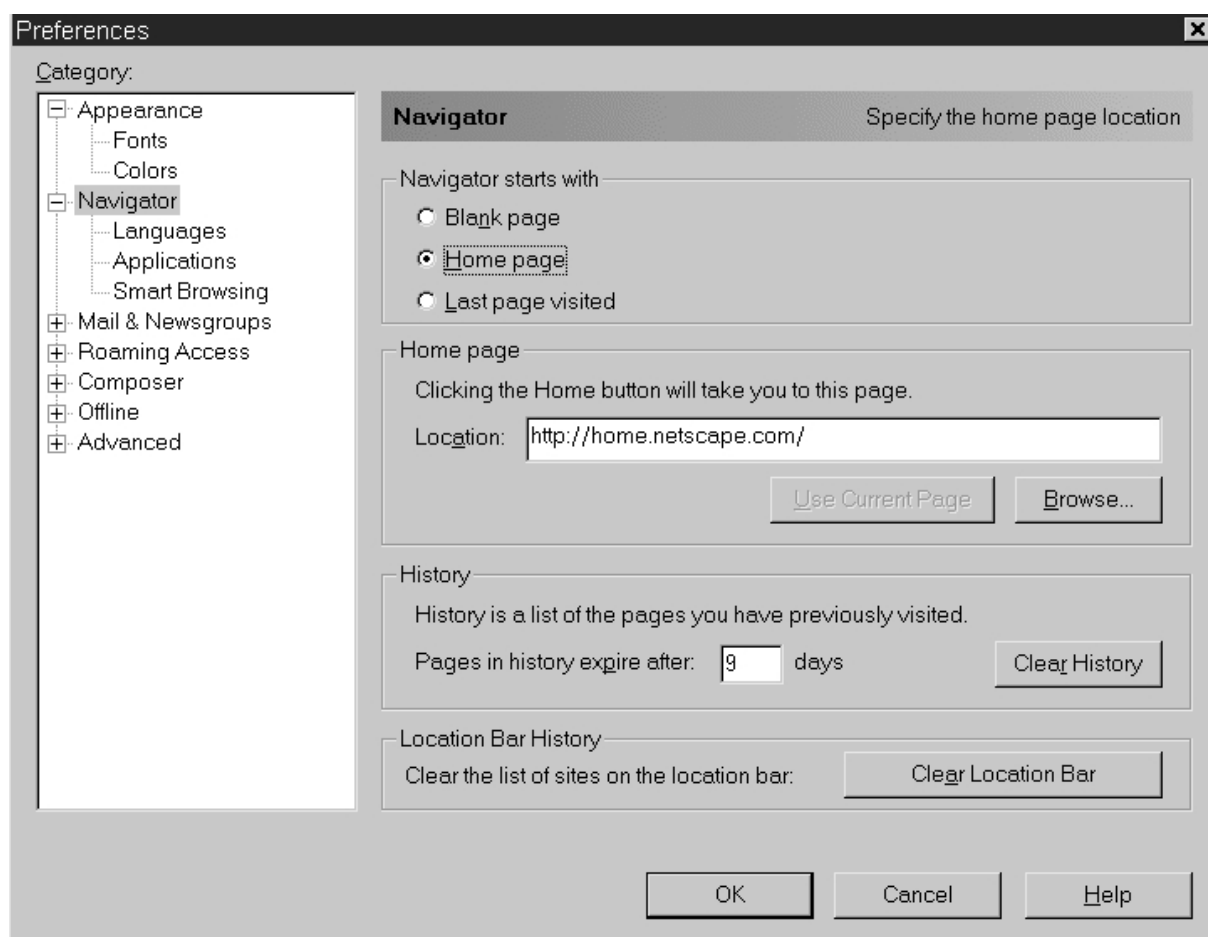
Una vez que se ha instalado una versión fiable del navegador, conviene dedicar algunos minutos a su configuración en vez de lanzarse a navegar directamente con las opciones por defecto con las que arranca el programa recién instalado.

El hecho de que exista en Netscape Communicator un menú con el nombre Información sobre seguridad puede confundir a los usuarios al inducirles a creer que basta con entender y configurar correctamente lo que aparece en dichos menús para garantizar la navegación segura. Como se verá a continuación, existen otras muchas opciones repartidas por diferentes menús que no deben dejarse al azar.

El recorrido por las opciones de seguridad de Netscape Communicator comenzará por la configuración de las **preferencias**. Para ello, se acude al menú de Edición y cuando se despliegue, se pulsa el comando Preferencias.... Las opciones seleccionadas se salvan en un archivo localizado en su directorio personal dentro de Netscape. Por ejemplo, una localización típica sería C:\Archivos de programa\Netscape\Users\gonzalo\prefs.js.

Carpeta Navigator

En la carpeta Navigator se ofrece la posibilidad de configurar el número de días que las páginas web visitadas aparecerán listadas en la ventana de historial. Esta ventana contiene el URL o dirección de todas las páginas que se han visitado durante el número de días especificado. En el caso de formularios, aparecerá incluso el contenido que se escribió en ellos. En otras palabras, cualquier persona que accediera a esta información sabría qué páginas han sido visitadas, cuándo y, en el caso de los formularios, qué datos se le proporcionaron. Desgraciadamente, errores de seguridad en este navegador, permiten a cualquier sitio de Internet obtener esta información de los usuarios que lo visiten. Si no quiere que caigan en otras manos, debe establecer a cero los días



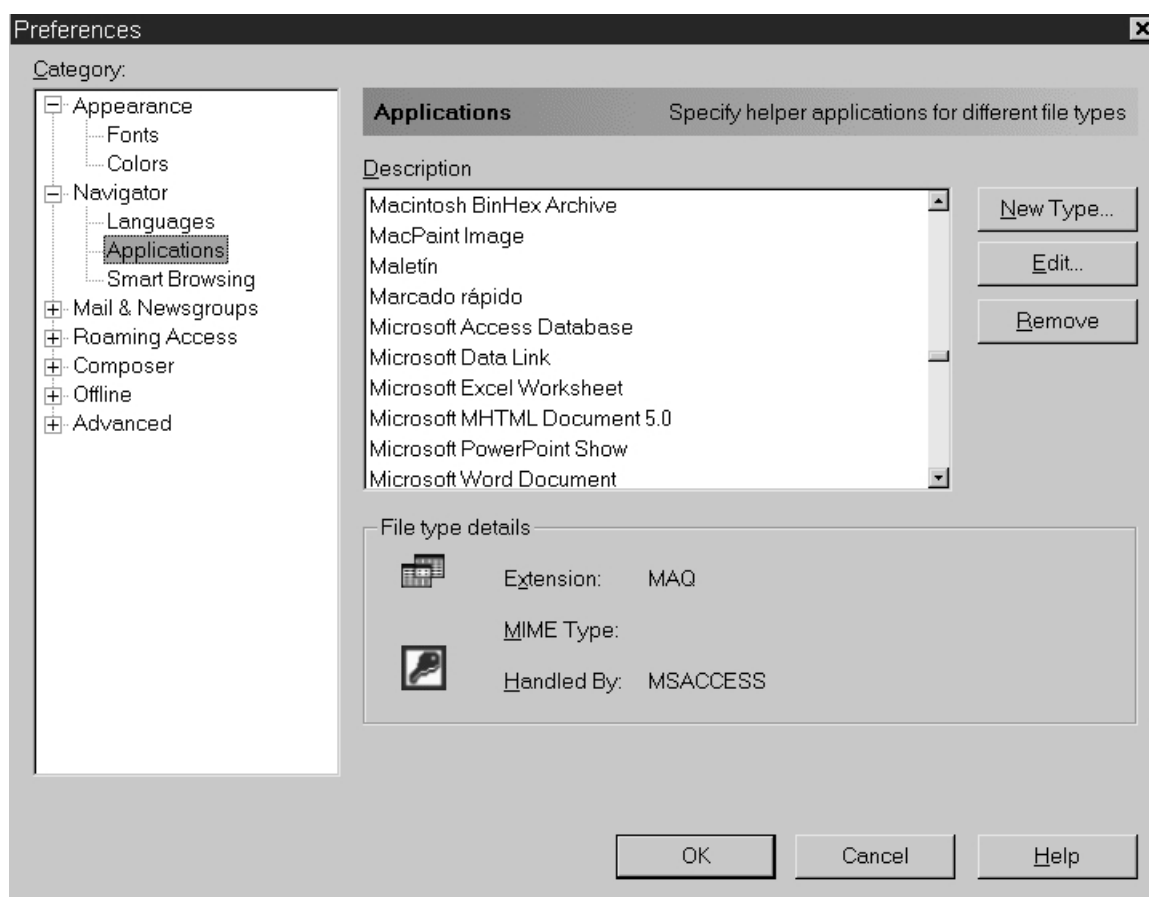
Puede asimismo hacer la siguiente prueba: escriba

about:global

en la ventana de dirección y compruebe cómo aparece en la ventana del navegador la lista completa de los últimos sitios que ha visitado. Observe cómo si rellenó algún formulario, también aparecerán los datos suministrados (siempre y cuando el método de envío de datos del formulario fuera GET).

En la versión 4.5 aparece además la opción de limpiar el contenido de la barra de dirección (los sitios que aparecen en una lista desplegable al pulsar la flecha de la derecha). Al igual que en el caso anterior, se muestran las direcciones de las páginas más recientemente visitadas, con la posibilidad de que cualquiera que se siente a continuación las vea, sabiendo qué sitios visitó recientemente.

Bajo la opción de Aplicaciones se puede especificar qué aplicaciones de ayuda y plug-ins se lanzarán en respuesta a la carga de ficheros con una extensión determinada y un tipo MIME asociado que el navegador no puede visualizar directamente. Así, por ejemplo, si al navegar por una página web encuentra un enlace a un documento Word, cuya extensión es .doc, al seguir el enlace se arrancará Microsoft Word, si así aparece configurado en la ventana de aplicaciones. Esta característica permite que el navegador sea capaz de visualizar directamente documentos en PDF, archivos de sonido o de vídeo, etc.



Tanto las aplicaciones de ayuda como los plug-ins son programas en código nativo con acceso total a los recursos del sistema, por lo que conviene instalarlos con precaución, ya que si alguno estuviera escrito con malas intenciones podría causar daños irreparables. De hecho, se han producido ataques gracias a plug-ins maliciosos

Otros plug-ins, sin estar específicamente diseñados para perjudicar al navegante, contenían agujeros de seguridad que permitían obtener información de su sistema, como ocurrió en 1997 con el plug-in de ShockWave de Macromedia, que permitía a un servidor web obtener ficheros del disco duro del visitante. O el problema con Flash a comienzos de 2001 o con Media Player.

Por otro lado, una página maliciosa podría también utilizar documentos que contuvieran virus de macro, como ha ocurrido en Word y Excel, para hacer que el usuario los ejecutara.

Como medida cautelar, se debe instalar el menor número posible de plug-ins y aplicaciones de ayuda y siempre de casas conocidas en las que se puede confiar. Para los tipos de archivo que se consideren potencialmente portadores de virus o con capacidad de interpretar comandos, se debe especificar que el navegador pida confirmación antes de abrirlos. Para ello, se selecciona el tipo de documento, por ejemplo "Microsoft Excel Worksheet" y se aprieta el botón de Editar... en la ventana que aparece. En la nueva ventana se selecciona la opción de avisar antes de abrir documentos de este tipo.

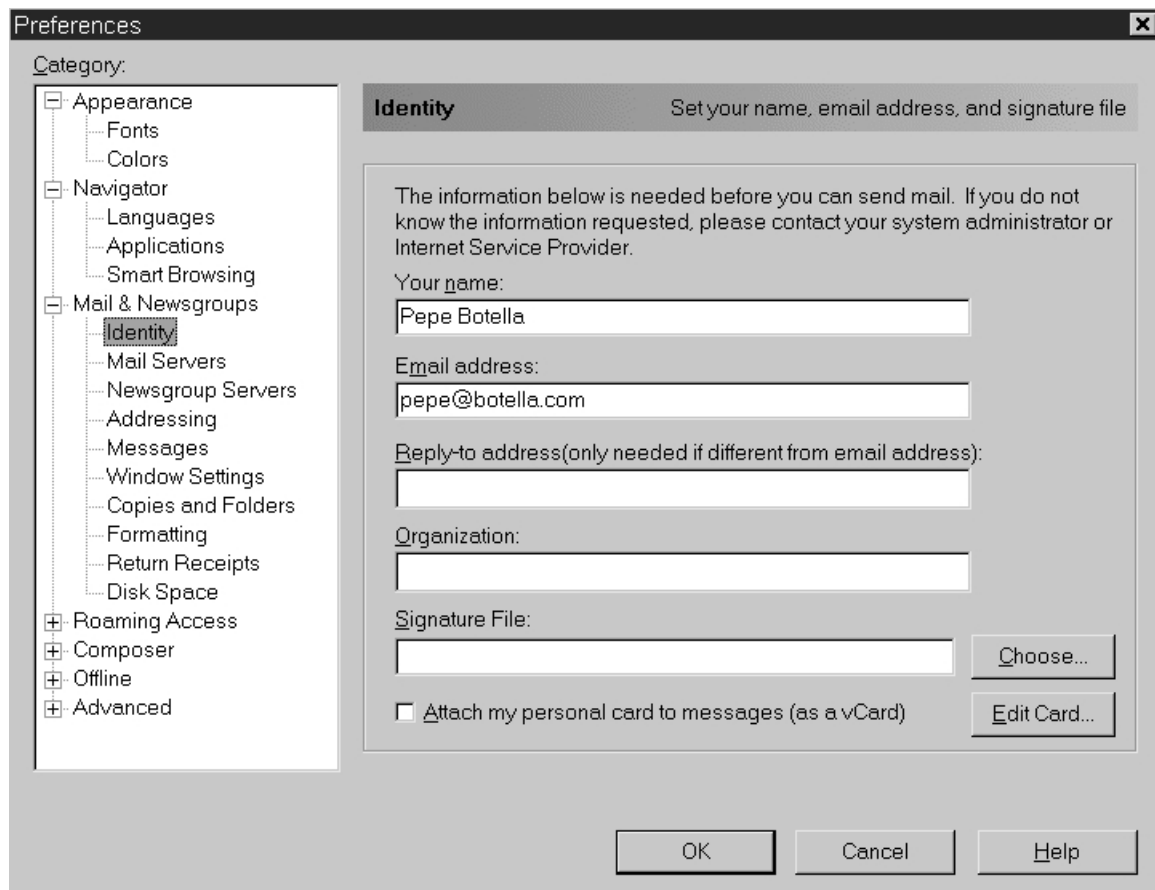
Puede comprobar qué plug-ins tiene instalados escribiendo en la ventana de dirección:

about:plugins

Es muy probable que se sorprenda de la cantidad de plug-ins que posee, sin ser consciente de ello. ¿Quién los puso ahí? Usted, cuando instaló otros programas, que a lo mejor en algún momento de la instalación le interrogaron acerca de su deseo de añadir un programa para su integración con el navegador.

Carpeta Correo y Grupos

Existen ciertos aspectos con relación al correo que conviene tener en cuenta a la hora de proteger la intimidad. El primero de ellos y uno de los más importantes concierne a la identidad del usuario. En la opción Identidad se puede especificar el nombre y dirección de correo del usuario, entre otros datos.



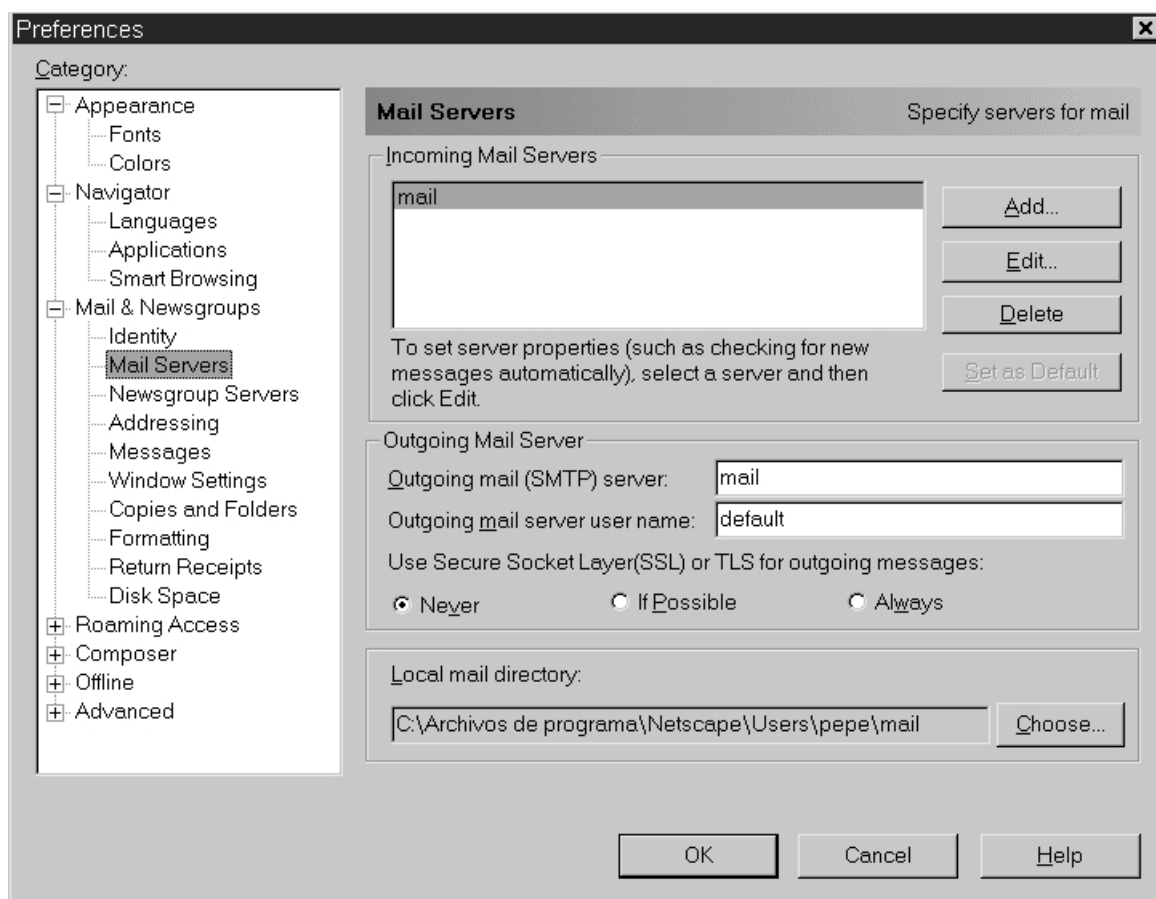
Si se utiliza Netscape como cliente de correo, evidentemente estos datos deben ser ciertos para poder enviar y recibir mensajes. Sin embargo, existen técnicas que permiten obligar al visitante de una página a enviar un correo sin que se dé cuenta, por el mero hecho de pasar el ratón sobre una imagen o cargar una página. En este caso, se enviará el correo con la dirección y nombre introducido en esta ventana. En las versiones de Communicator 4.x, antes de enviar el correo se le pide confirmación al usuario, pero son muchos los usuarios que bien porque han adquirido el hábito de decir que sí a todo, bien porque no entienden o no leen el contenido de la ventana de confirmación, lo cierto es que envían su dirección indiscriminadamente.

Siempre se debe leer atentamente cada ventana que aparece antes de emprender acciones que puedan comprometer la seguridad.

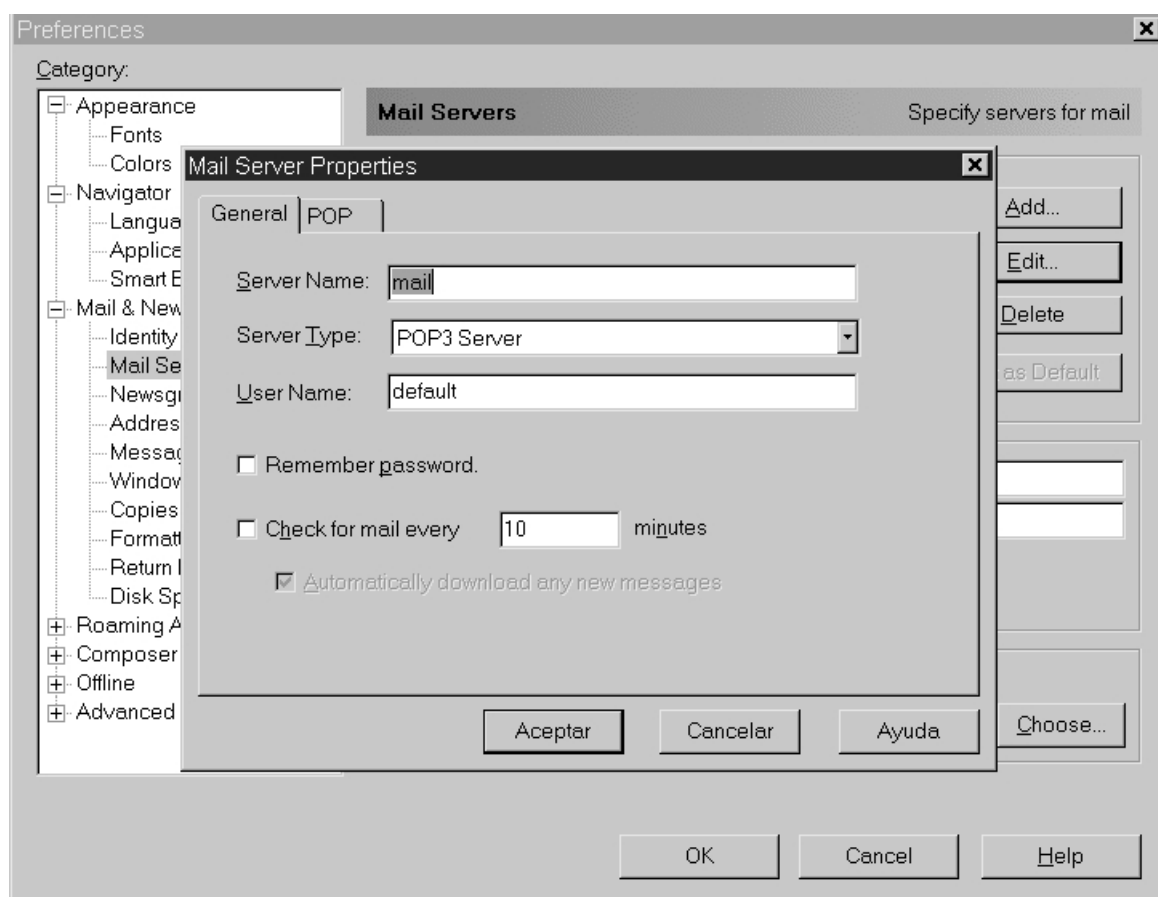
Algunos usuarios introducen datos falsos, lo cual puede ser una buena idea para contrarrestar el problema anterior.

La opción Servidor de correo permite determinar el lugar del disco duro donde se almacenará todo el correo recibido, enviado, borrado, etc. Normalmente, existe un lugar por defecto que conviene cambiar, ya que existen muchos agujeros en los navegadores que facilitan a sitios web remotos el examen del contenido de archivos en el disco duro cuyo nombre y localización se conocen.

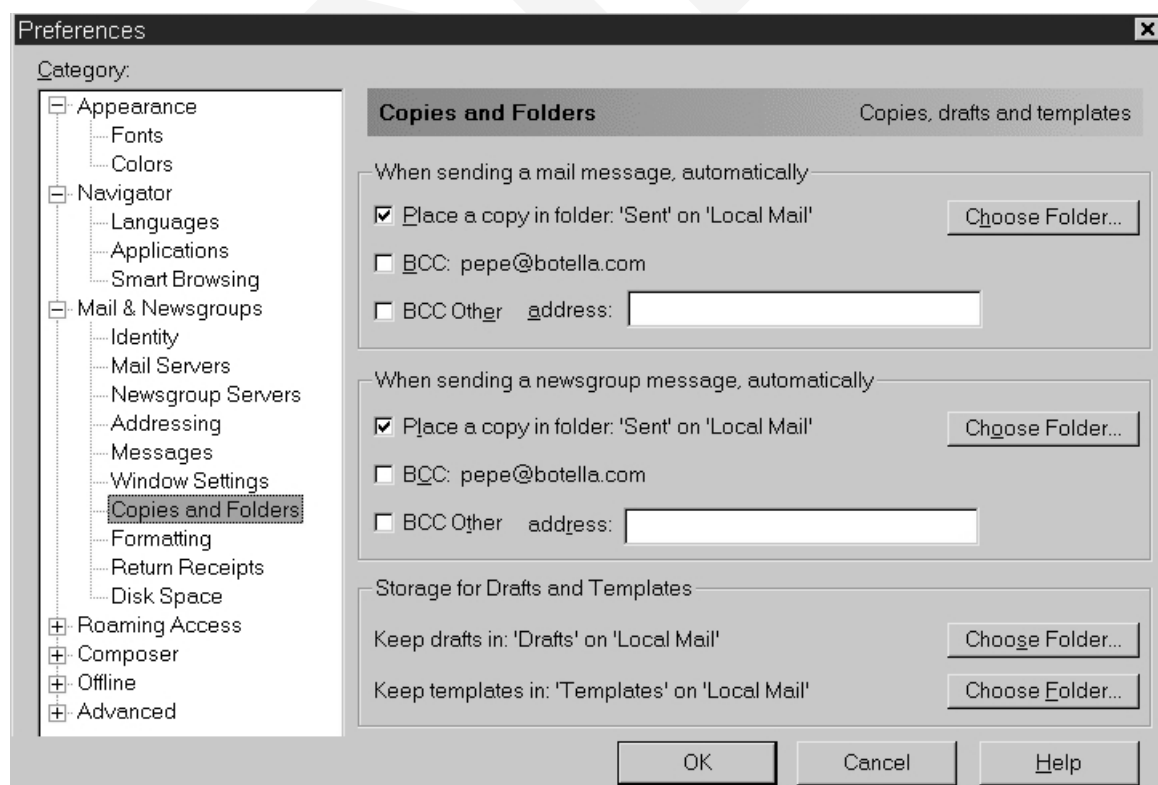
Si uno no se molesta en cambiar el lugar donde se guarda todo el correo, cualquier servidor web que se interese en ello puede leerlo, tanto el enviado como el recibido. No cuesta nada cambiar la localización por defecto a otro lugar en el disco duro y añadirá seguridad.



También se ofrece la posibilidad de guardar la contraseña de acceso al servidor de correo. Piense que si activa esta casilla, cualquier persona con acceso a su navegador podrá leer los futuros correos que reciba mientras usted no esté presente, mientras que en caso contrario, se le pedirá la contraseña cada vez que inicia una nueva sesión con el servidor.



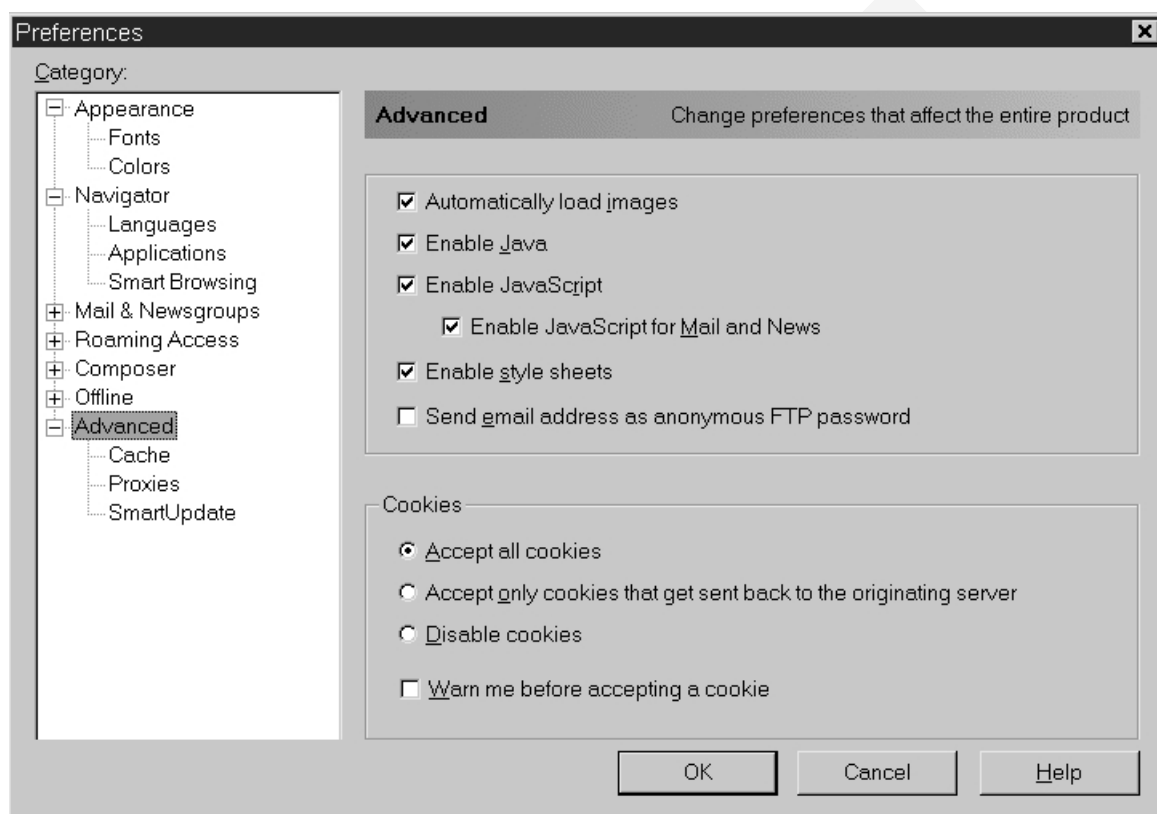
En la opción Mensajes en las versiones 4.0x y Copias y carpetas en 4.5, se ofrece la posibilidad de enviar a terceras personas copias de los correos mandados al exterior.



También existe la posibilidad de especificar dónde se almacenarán los correos enviados, si es que se quieren guardar en disco. Nunca hay que perder de vista el hecho de que en sistemas Windows, siempre que no se utilice alguna herramienta de cifrado, cualquiera puede acceder al contenido del disco duro, por lo que se podría leer el contenido de los correos. Si no se cambia el directorio por defecto donde se almacenan, como se ha explicado anteriormente, entonces no sólo las personas con acceso físico al ordenador, sino cualquier máquina conectada a Internet podría leerlos explotando algunos de los agujeros del navegador.

Carpeta Avanzadas

Por defecto, Java y JavaScript aparecen activados tras la instalación del programa. Si no ha modificado la configuración de su navegador, puede comprobar cómo las casillas se encuentran activadas.



Java y JavaScript son lenguajes de programación que añaden inteligencia y realzan el contenido de las páginas web. Hoy en día, son pocas las páginas que no hacen uso de una u otra forma de programación. Por desgracia, la gran mayoría de agujeros de seguridad que se han descubierto en Netscape están directamente relacionados con la forma de implantarse estos lenguajes en el navegador. En espera de parches o nuevas versiones mejoradas, el consejo habitual para los navegantes es que se desactive Java y JavaScript como medida preventiva. Si alguien se siente amenazado, lo puede hacer desactivando las casillas anteriores.

En la ventana aparece también la opción de enviar la dirección de correo como contraseña de FTP. El protocolo de transferencia de ficheros (FTP) se utiliza para transferir ficheros voluminosos a través de Internet. Normalmente se accede a servidores anónimos que piden como contraseña la dirección de correo del cliente. Los navegadores incorporan entre los protocolos que soportan el citado FTP, de manera que se encargan automáticamente de recuperar ficheros a través de este protocolo sin que el usuario

tenga que hacer nada especial además de pulsar sobre un simple enlace. Aprovechándose de esta técnica, algunos sitios web insertan en sus páginas imágenes u otros elementos que se recuperan a través de FTP, en vez de utilizar el protocolo convencional HTTP, de manera que si la opción de suministrar la dirección de correo como contraseña estaba activada en el navegador, se harán con la dirección electrónica del usuario. Para prevenir este tipo de ataque encubierto, conviene desactivar la casilla.

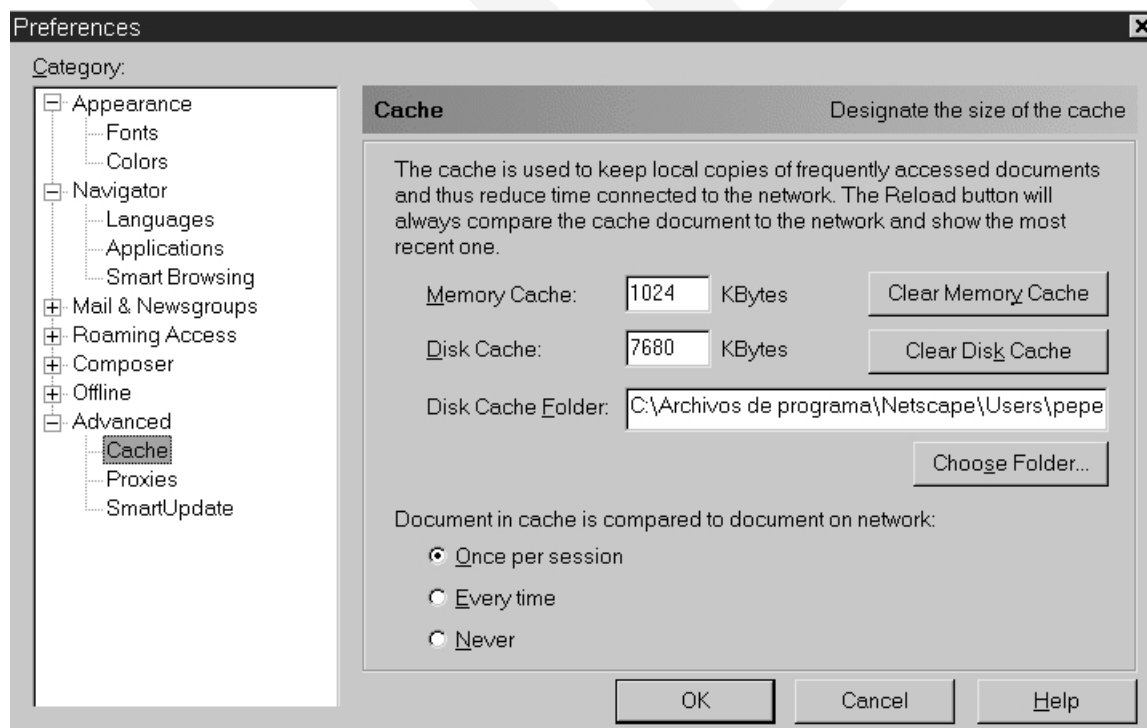
Las cookies son esos pequeños ficheros de texto que se almacenan en su disco duro con información que algunos servidores Web escriben ahí. Por defecto, está activada la opción de aceptar todas las cookies. Ahora bien, ¿resulta peligroso aceptar cookies? En principio, las cookies no revisten ninguna amenaza para la seguridad; sin embargo, utilizadas por ciertas compañías sin escrúpulos, pueden ayudar a la confección de perfiles de usuario y hábitos de navegación, básicamente con el fin de dirigirles propaganda personalizada.

No obstante, seleccionar la opción de deshabilitar las cookies puede conducir a que muchos sitios web no se visualicen correctamente o con sus plenas capacidades, como ocurre por ejemplo con el uso de carritos de la compra o la configuración personalizada de servicios (por ejemplo, la web de venta de libros amazon.com).

Por otro lado, debido al uso masivo de cookies que hacen algunos servidores web, seleccionar la casilla de avisar antes de aceptar cookies puede acabar inundando al navegante con ventanas de aviso de cookies. Por lo tanto, como solución intermedia, se recomienda aceptar todas las cookies en aquellos sitios de confianza, con una política de privacidad claramente establecida y deshabilitarlas en el resto.

Los navegantes más intrépidos pueden instalar algún programa que permita un filtrado selectivo de cookies en función del servidor que las envía.

Bajo la opción Cache se pueden configurar los aspectos relacionados con la cache donde se almacenan temporalmente las páginas e imágenes visitadas más recientemente.



Si bien su función primaria es aumentar la velocidad de navegación, leyendo las páginas ya visitadas desde la cache en lugar de descargarlas de nuevo a través de la Red, en la práctica se puede explotar para conocer las idas y venidas de un navegante, ya

que contiene cada página e imagen que vio, los archivos de audio que escuchó, etc. Por esta razón, conviene en primer lugar cambiar el directorio por defecto donde se almacena.

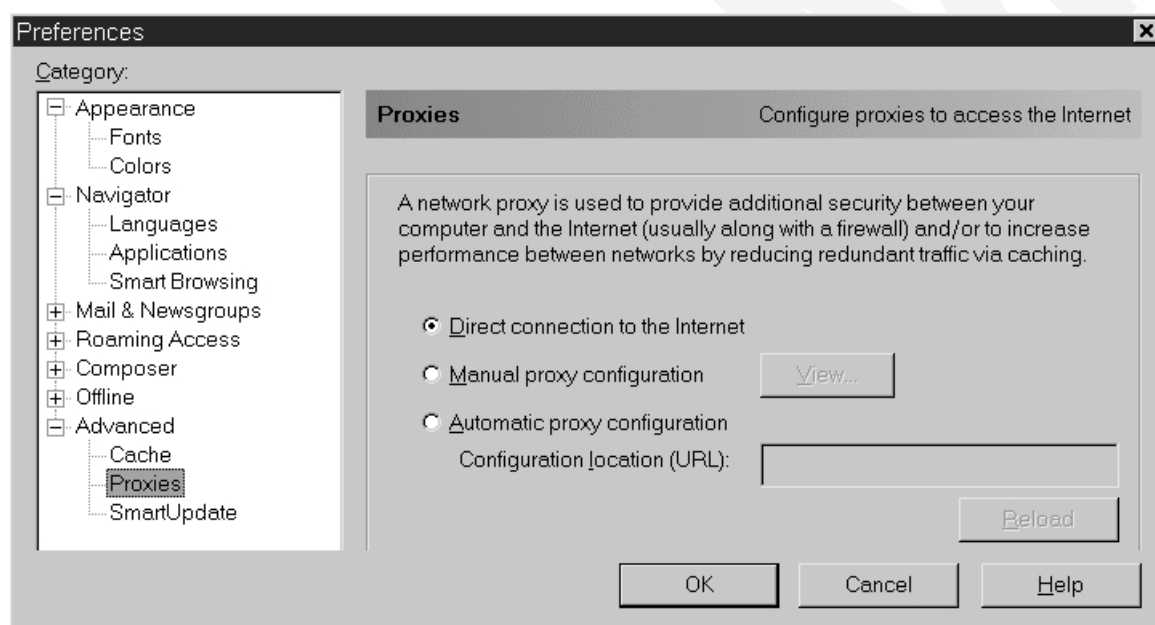
En segundo lugar, para los usuarios más preocupados por su intimidad, se puede poner a cero de manera que nada se almacene en el disco. Puede hacer la siguiente prueba: escriba

about:cache

en la ventana de dirección y compruebe cómo aparece en la ventana del navegador la lista completa de los últimos sitios que ha visitado, imágenes cargadas, documentos Word o PDF leídos, presentaciones en PowerPoint visualizadas, etc. Para comprobar el cache de memoria, puede escribir en la ventana de dirección:

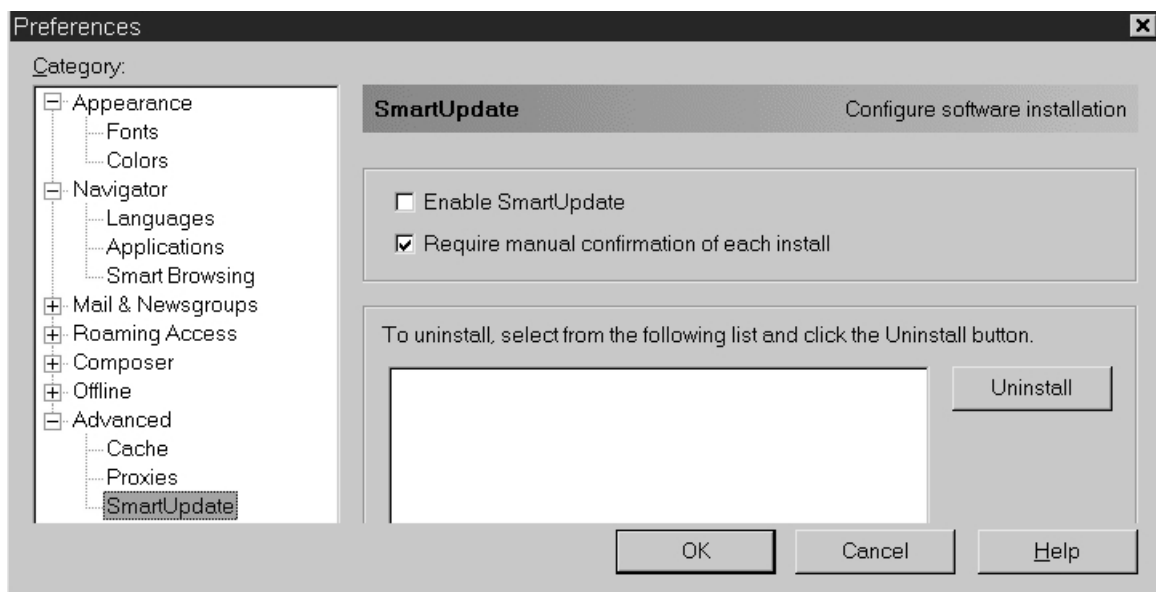
about:memory-cache

Bajo la opción Proxies encontrará todas las opciones para configurar el funcionamiento del proxy. La idea básica de un servidor proxy es actuar de pasarela (gateway) entre su máquina o su red e Internet.



Normalmente se usan para llevar las peticiones del cliente a través de un cortafuegos (firewall): el proxy espera a una petición desde dentro del cortafuegos y la reexpide al servidor remoto en el exterior del mismo, lee la respuesta y la envía de vuelta al cliente. Dado que todas las peticiones pasan a través del proxy, si un atacante introdujera en su configuración sin que se diera usted cuenta la dirección de un servidor proxy correspondiente a una de sus máquinas, este servidor registraría todos los sitios que visita y los datos que introduce en los formularios. Por otro lado, siempre que navegue a través de un proxy, los servidores web verán la dirección del proxy y no la de su máquina, por lo que los proxies pueden ser utilizados para la navegación anónima.

Autoinstall/SmartUpdate. A partir de las versiones 4.x es posible instalar automáticamente los plug-in necesarios para visualizar ficheros especiales.



Aunque representa una opción muy cómoda para el navegante, se recomienda desactivar la casilla de permitir la autoinstalación en las versiones 4.0x (en la carpeta de Avanzadas), mientras que se debe activar la casilla de solicitar confirmación manual para cada instalación en la versión 4.5. No le conviene que ningún tipo de software se instale en su ordenador sin su conocimiento.

Netwatch

NetWatch es la protección basada en restricciones por contenidos incorporada por Netscape Navigator 4.5, que le permitirá controlar qué clase de páginas web se pueden visualizar en su ordenador.

NetWatch de Netscape utiliza el estándar de clasificación conocido como PICS. NetWatch reconoce dos sistemas de clasificación independientes compatibles con PICS: RSACi, y SafeSurf. Cada sistema emplea un método diferente para describir con el mayor detalle posible los niveles de contenido potencialmente ofensivo en las páginas web. Estos contenidos se agrupan en las siguientes categorías: violencia, desnudez, sexo y lenguaje. SafeSurf añade, además, otros contenidos, como profanidad, heterosexualidad, homosexualidad, intolerancia racial, sexual o religiosa, drogas, juego, etc.

Una vez que la protección de NetWatch ha sido activada, cuando se accede a una página con Netscape Navigator, NetWatch compara la clasificación de la página con los niveles que han sido configurados como aceptables y si todos los niveles de la página son inferiores se permite su visualización. También se puede bloquear todas las páginas que carezcan de clasificación, si bien esta opción limitaría drásticamente la navegación por Internet, ya que son muy pocas las páginas que actualmente incorporan clasificación.

Con el fin de evitar que otros usuarios vean o cambien su configuración, ésta se protege mediante una contraseña. A partir del momento en que se activa la protección de NetWatch, nadie que use su navegador podrá saltársela.

Puede configurar NetWatch si lo desea, seleccionando el comando NetWatch del menú Ayuda.