[Capítulo 3]

Navegador

Cambiar el navegador: Firefox

Existen multitud de razones por las que no es deseable utilizar *Internet Explorer* para navegar a través de Internet sino otros navegadores. Es especialmente recomendable el uso de *Firefox*, un navegador de código abierto. *Firefox* es el heredero de *Netscape Navigator*, un navegador que tuvo un uso masivo hasta que fue superado por *Internet Explorer*. En 1998 Netscape publicó gran parte del código de *Netscape Communicator* y se creo una organización llamada *Mozilla* para desarrollar esta aplicación. Poco después se abandonó todo el código existente para reescribir el navegador desde cero. En estos años se han hecho grandes avances en el desarrollo de *Firefox* y hoy en dia es, probablemente, el más avanzado de los navegadores existentes.

Porqué debería usar Firefox en lugar de Internet Explorer?

- **Mejor soporte de estándares:**
  Firefox soporta más estándares y lo hace mejor que *Explorer*. De esta forma, cualquier página que este bien construida se verá correctamente en *Firefox*, lo cual no siempre sucede con *Explorer*, que además suele implementar extensiones propietarias que ningún otro navegador soporta.

- **Seguridad:**
  Firefox es mucho más seguro que *Internet Explorer* ya que está pensado, desde un principio, para ofrecer la máxima seguridad al usuario. Por ello, no permite la instalación o ejecución de código bajado de Internet sin el consentimiento del usuario así como tampoco el uso de controles *ActiveX*, una de las causas más habituales de los fallos de seguridad de *Internet Explorer*. Además, *Firefox* no implementa el concepto de zonas del que dispone *Explorer*, de forma que trata todo el contenido al que puede acceder como potencialmente peligroso, sin darle la posibilidad de otorgarle más permisos, otro de los fallos habituales de *Explorer* del que se aprovechaba mucho código malicioso para cambiar de zona y conseguir más privilegios.

- **Multiplataforma:**
  Firefox no solo funciona bajo *Windows*, sino que además también lo hace bajo *Linux*, *Mac OS X* y *Solaris*. Además, está disponible en multiples idiomas, como puede ser castellano, catalán, gallego y muchos otros.

- **Extensible y adaptable:**

  Firefox provee de diversos métodos para cambiar la funcionalidad y la apariencia del navegador. A través de las extensiones podemos conseguir nuevas funciones del navegador, como bloqueo de publicidad o pequeños juegos. También podemos cambiar la apariencia del navegador mediantes los Temas, los conocidos *skins* que permiten cambiar desde los iconos hasta cualquier otro detalle del navegador.

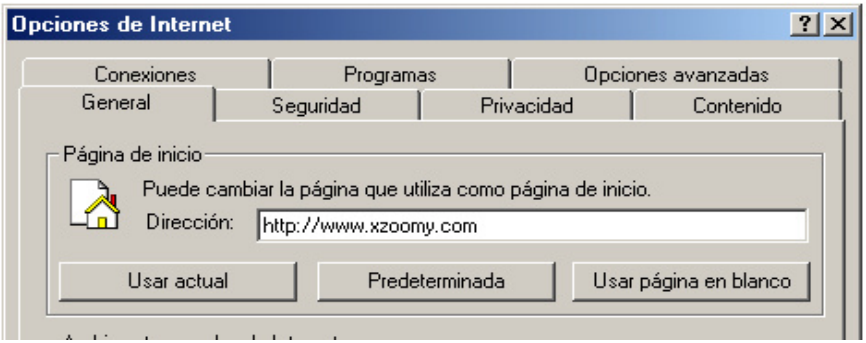
- **Garantía de reembolso:**

  Además de todo esto, *Firefox* es gratuito y ocupa menos de 5 Mb, por lo que no perdemos nada por probarlo. Es probable que una vez lo hayamos probado ya no queramos volver nunca más a usar Internet Explorer.

Hijack

Una método utilizado por algunas páginas para aumentar el número de visitas que reciben es el *browser hijacking*, que consiste en el uso de técnicas para modificar algunos aspectos de nuestro navegador, como, por ejemplo, nuestra página de inicio o la de búsqueda.

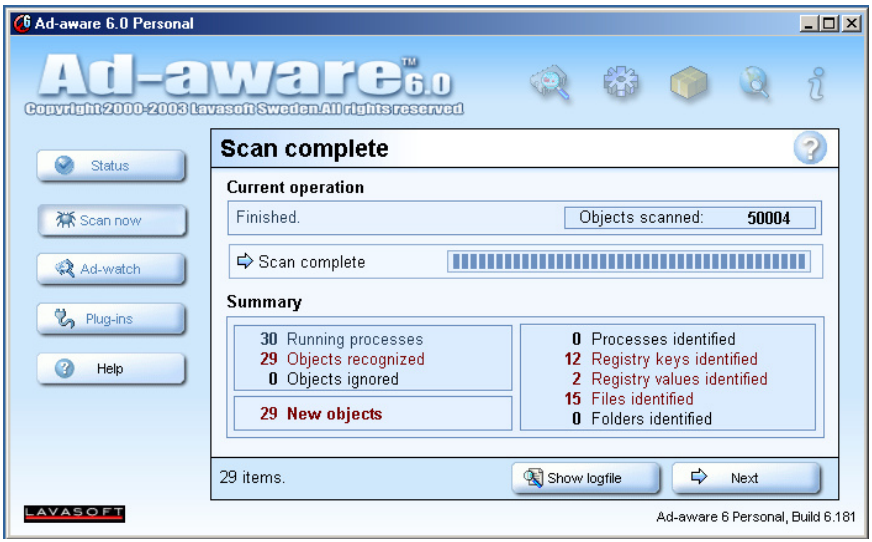
Qué se consigue con esto? Por una parte, aumentar el tráfico que recibe esa página, cosa que hará aumentar los beneficios por publicidad gracias a los *banners* que contendrá. Otras páginas lo utilizan para rastrearnos y espiar las páginas que visitamos, para crear perfiles sobre nosotros.



Existen diferentes tipos de técnicas para lograr estos objetivos. La menos peligrosa consiste en añadir un link a nuestros favoritos con el objetivo de que lo visitemos. También suelen modificar la página de inicio, de forma que cada vez que iniciemos el navegador iremos a parar a su sitio. Otros sitios más agresivos modifican nuestra página de búsqueda de modo que nuestro buscador por defecto será el suyo; algunas incluso nos harán creer que el buscador utilizado habitualmente (Google, Yahoo,...) funciona correctamente, pero los resultados ofrecidos no serán correctos, apuntando en su mayoría a su página. Finalmente, las más peligrosas llegan a modificar el

registro de Windows, a deshabilitar las opciones de Internet o a instalarnos programas de forma que cuando reiniciemos el ordenador los cambios que han hecho se mantengan. Para poder recuperar nuestro navegador, en un principio nos servirá el mismo programa que utilicemos para eliminar el spyware, por ejemplo *Ad-Aware* o *SpyBot* .

En caso de que con estos programas no consigamos recuperar el control de nuestro navegador podemos utilizar otros más avanzados como *Hijack This*, cuyo uso es más complicado pero nos asegurará el borrado de cualquier hijacker.



Parásitos

Cuando navegamos por Internet podemos encontrarnos miles de parásitos que intentan entrar en nuestro ordenador, normalmente a través de nuestro navegador, para lograr su propósito: instalarse en nuestro sistema. El objetivo de todos estos parásitos suele ser que veamos publicidad (a veces, incluso, redirigiendo las peticiones de páginas que hacemos hacia su propio servidor) o recopilar datos sobre nuestros hábitos de navegación.

Existe una manera sencilla y eficaz de evitar que la mayoría de estos bichos entren en nuestro sistema y es a través del fichero HOSTS. Cómo funciona este método? En primer lugar deberemos saber como funciona el sistema de DNS. En Internet cada servidor se identifica por su dirección IP, una serie de números que vienen a ser equivalentes al número de teléfono del servidor. Pero nosotros estamos acostumbrados a escribir una dirección textual; aquí es donde entra en juego el DNS. El DNS es el sistema encargado de convertir una dirección (p.ej. www.elligre.tk) en su correspondiente dirección IP (69.93.4.26). Así, solo nos falta saber que la dirección 127.0.0.1 corresponde siempre a nuestro propio ordenador, el que estemos utilizando en ese momento.

El fichero HOSTS le indica al sistema operativo la dirección IP correspondiente a ciertas direcciones textuales. Si en este fichero le indicamos 127.0.0.1 como dirección IP de un cierto sitio, el navegador no será capaz de encontrar ese sitio, ya que lo intentará buscar en nuestro ordenador local y no encontrará nada. Así, podemos aprovechar para bloquear todos aquellos sitios a los que no queramos acceder.

Para conseguir esto simplemente deberemos bajarnos el fichero HOSTS de alguna de las siguientes páginas:

http://www.mvps.org/winhelp2002/hosts.htm
http://www.everythingisnt.com/hosts.html
http://pgl.yoyo.org/adservers/

y deberemos guardarlo en el directorio `c:\windows\system32\drivers\etc` (puede ser diferente si tenemos el sistema operativo instalado en otro directorio). A partir de ese momento navegaremos más seguro y más rapidamente, sin tener que ver tanta publicidad en nuestro navegador.

Alguno de estos ficheros HOSTS solo bloquea la publicidad y no el resto de parásitos, por ello el más recomendable es el que está disponible en el primero de los links. De todas maneras, podemos probar cual nos gusta más, ya que cada uno bloquea sitios diferentes.

Cookies

Qué son las cookies?

El protocolo HTTP, que es el que usa nuestro navegador, es un protocolo sin estado, es decir, que no guarda ninguna información entre una petición de una página y la siguiente. Esto impide al servidor saber si quien pide una página es el mismo que ha pedido otra anteriormente, lo que provoca que el servidor no tenga manera de guardar preferencias o datos similares para personalizar las páginas que se le piden.

Por ejemplo, en el buscador Google podemos personalizar las búsquedas indicandole en que idioma queremos buscar o cuantos resultados queremos visualizar por pantalla. Como se consigue esto? A través de las *cookie*s.

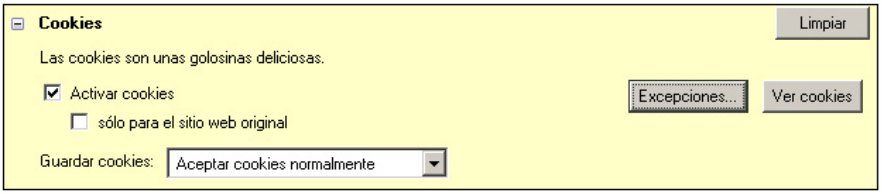
Las *cookies* son unas pequeñas cadenas de texto que nos envía el servidor la primera vez que nos conectamos a él. Esta cadena nos identifica ante el servidor, ya que cada vez que pedimos una página a ese servidor se envía de vuelta la *cookie*, de forma que pueda saber quien somos.

El problema de las cookies

Esto puede ser bueno en determinadas páginas, pero presenta un problema cuando se usa indebidamente. Muchas empresas de publicidad instalan *cookies* en nuestro ordenador sin avisarnos, de forma que pueden conocer que páginas visitamos y de este modo enviarnos publicidad personalizada. Hay que tener en cuenta que las *cookie*s no pueden dañar nuestro ordenador (como haría un virus), pero pueden dañar nuestra privacidad si son usadas incorrectamente

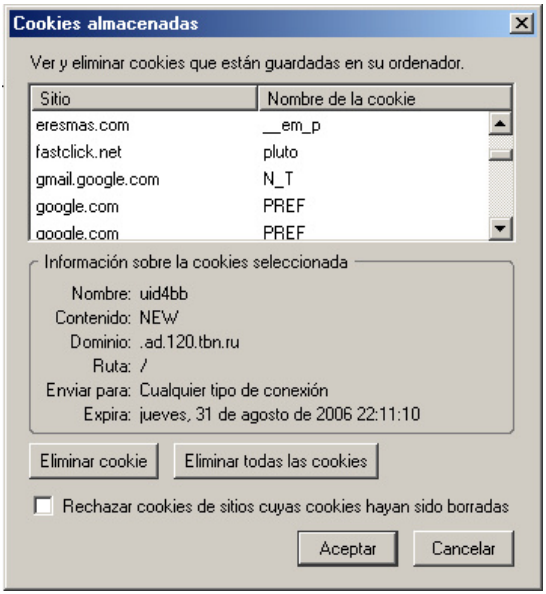
por parte del servidor; no todas las *cookies* son malas y algunas son muy útiles.

La forma más sencilla de librarse de ellas es desactivándolas en nuestro navegador o bien configurando que sitios permitimos que nos envíen cookies y cuales no. Para ello, en Firefox podemos ir al menú Herramientas -> Preferencias y allí ir a la opción de Privacidad, donde encontraremos el apartado Cookies.



Desde allí podemos desactivarlas o establecer excepciones, de forma que podremos indicarle al navegador las páginas de las que no queremos recibir *cookies*. Es recomendable, además, activar la opción *Sólo para el sitio web original*, para evitar que diferentes sitios web puedan enviarse sus *cookies* entre ellos

También podemos ver todas las *cookies* que ya tenemos en nuestro ordenador si pulsamos en la opción *Ver cookies*. Desde allí podremos borrarlas individualmente o todas de una vez.



Debemos tener cuidado con las *cookies* que borramos, ya que al eliminar algunas de ellas podemos perder la configuración personalizada o la entrada automática (sin tener que introducir el usuario y la contraseña) en alguna de las webs que visitemos habitualmente. Por ello, es recomendable borrar solo aquellas que sean procedentes de sitios que no conocemos o que sepamos que no vamos a visitar con frecuencia.

HTTP Seguro

El protocolo HTTP, usado al navegar por Internet, envía todos los datos a través de la red en forma de texto. Esto implica que cuando estamos accediendo a cualquier página web todo lo que enviamos y recibimos puede ser leído por todos los ordenadores por donde pasan los datos (los de nuestro ISP, los del ISP de la página a la que accedemos, los nodos intermedios,...)

Cuando navegamos por páginas con información confidencial como, por ejemplo, nuestro correo electrónico o la página de nuestro banco, no queremos que esa información pueda ser leída por nadie, por lo que no nos interesa utilizar el protocolo HTTP habitual, sino el protocolo HTTP seguro, que permite, además de ocultar la información que se transmite, asegurar que la página a la que nos conectamos es quien dice ser y no ha sido suplantada por otra.

Cómo funciona HTTP Seguro?

HTTP Seguro (a partir de ahora, HTTPS) funciona gracias a la criptografía, que permite asegurar mediante una serie de funciones matemáticas el origen y la ocultación de los datos. Por suerte, no necesitamos saber como funciona matemáticamente el sistema, ya que el navegador se encargará automáticamente de ello.

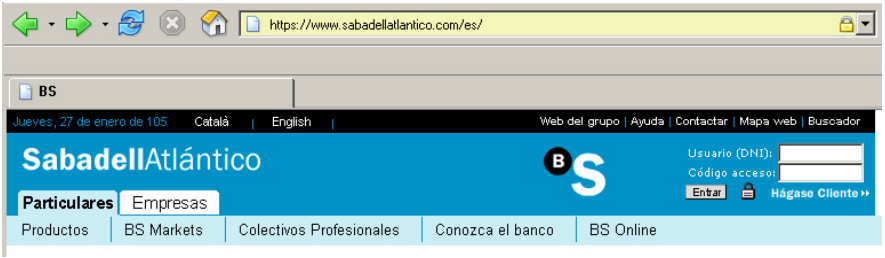
Cada servidor que quiera implementar HTTPS debe disponer de un certificado, una especie de DNI digital, que nos indica todos sus datos y la clave que permite cifrar todo lo que enviamos y recibimos del servidor. Estos certificados son emitidos por una serie de compañías a nivel mundial, que garantizan la identidad del propietario del certificado.

Cómo utilizar HTTPS?

Vamos a ver un ejemplo práctico del uso de HTTPS. Para ello, entraremos en la web de un banco cualquiera, en este caso Sabadell Atlántico y veremos como utilizar el protocolo seguro.

La primera diferencia entre el protocolo normal y el seguro es el uso de https para indicar que la conexión debe ser segura. Si queremos acceder a nuestro banco la dirección para mostrar la página principal es http://www.sabadellatlantico.com.

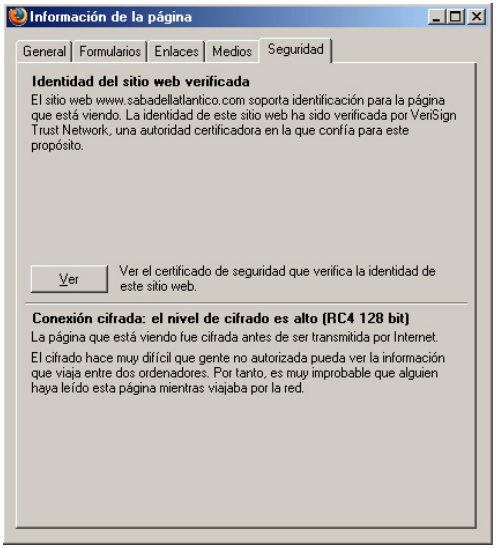
El problema de esta página es que la información enviada cuando intentemos conectarnos podría ser leída por otras personas y que no podemos asegurar el origen de la página, pues podría haber sido suplantada por alguien para intentar conseguir códigos de acceso al banco. Por ello, vamos a utilizar HTTPS para acceder a la página. En lugar de la dirección anterior, en esta ocasión cambiaremos el http del inicio por https, de forma que nos quedará https://www.sabadellatlantico.com y nos mostrará la misma página en modo seguro.



La segunda diferencia que encontramos en la página es que el navegador nos muestra la dirección con el fondo de color amarillo, para así poder distinguir las páginas normales de las seguras.

Finalmente, también se muestra un pequeño candado en la barra de la dirección y, si hacemos doble-click sobre él, se nos mostrará una ventana con información sobre la página actual, donde podremos comprobar la autenticidad del sitio y que la conexión ha sido cifrada de forma que nadie pueda leer nuestros datos. Podremos, Incluso, ver el certificado de la página para hacer comprobaciones más exhaustivas.

Es muy recomendable comprobar esta información cada vez que accedamos a una página segura, ya que el simple hecho de usar HTTPS no garantiza la autenticidad del origen de los datos, sino que debemos comprobarla personalmente. A pesar de eso, si la identidad del certificado no coincide con la de la página que estamos visitando el navegador nos avisará y nos mostrará una ventana con información, avisándonos de lo que sucede y preguntándonos si realmente queremos visitar la página.



ATENCIÓN

Acceder a un servidor en modo seguro no nos garantiza la fiabilidad de la operación que realicemos. Antes de realizar alguna compra a través de Internet es recomendable informarse acerca de la empresa que nos ofrece el producto. Normalmente, bastará con una simple búsqueda del nombre de la empresa en Google y allí podremos ver si hay alguna queja sobre su funcionamiento.

Referencias

Dirección de descarga de Firefox
http://www.difundefirefox.com/

Dirección de descarga de extensiones para Firefox
http://update.mozilla.org/extensions/

Dirección de descarga de temas para Firefox
http://update.mozilla.org/themes/

Dirección de descarga de HijackThis
http://tomcoyote.com/hjt/

Artículo muy completo acerca de las cookies
http://www.cookiecentral.com/faq/