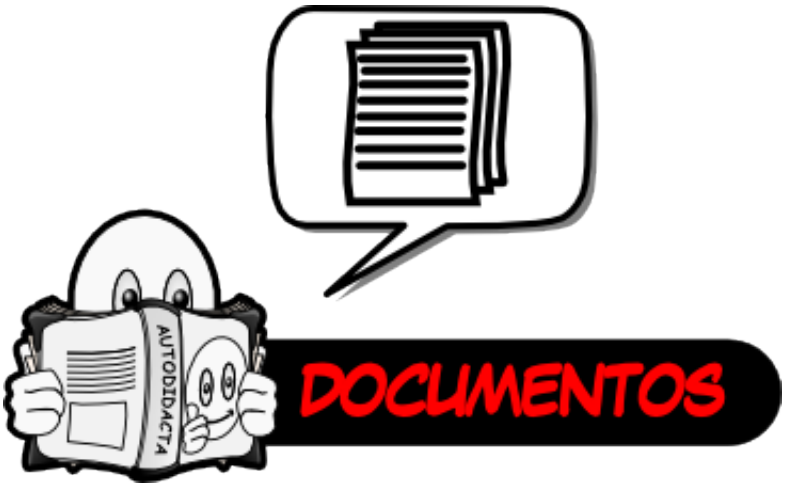
PROYECTO AUTODIDACTA

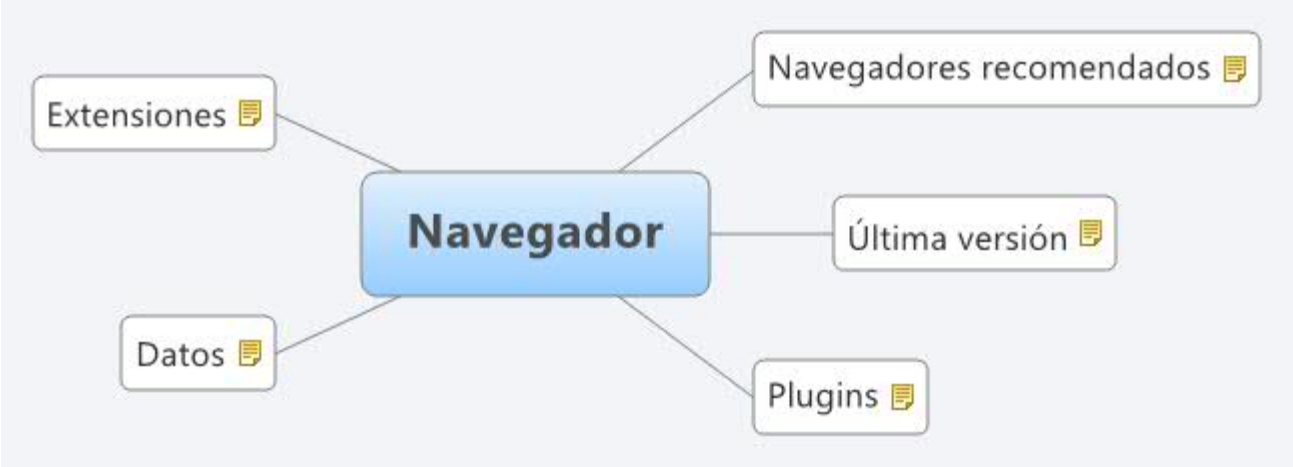
http://www.proyectoautodidacta.com



Precauciones al usar Internet

Precauciones al usar Internet

1. Navegador



1.1 Navegadores recomendados

1.- Firefox

2.- Opera

3.- Google Chrome

4.- Internet Explorer 7 o superior (aunque sigue fallando en seguridad)

1.2 Última versión

Emplea siempre la última versión de tu navegador favorito. Todos los días surgen nuevas amenazas en la red y por eso los navegadores se actualizan con bastante regularidad o frecuencia.

1.3 Plugins

Los plugins son pequeños programas que funcionan dentro de un programa más grande o principal. Los navegadores hacen mucho uso de los plugins, especialmente de los de Flash (para ver vídeos) y los de Java (para ejecutar programas). Procura siempre utilizar la última versión de estos, actualizada desde su sitio web original.

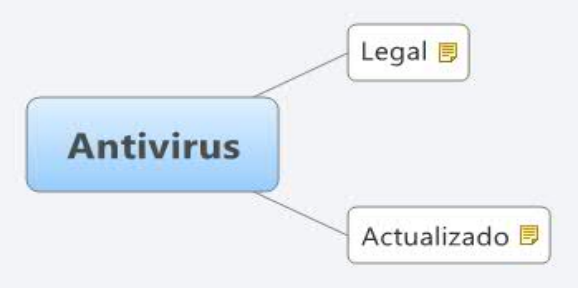
1.4 Extensiones

Las extensiones son muy similares a los plugins: pequeños programas que funcionan sólo dentro de uno más grande. Firefox cuenta con muchas extensiones y las actualiza automáticamente cuando es necesario. Siempre ten las extensiones actualizadas a la última versión.

1.5 Datos

En los navegadores se almacenan gran cantidad de datos que pueden ser susceptibles de ser robados o incluso de provocar problemas en el funcionamiento del programa. Cada cierto tiempo, borra el caché del navegador, el historial y las cookies (pequeños archivos que se colocan en nuestro equipo para almacenar información relativas a sitios web).

2. Antivirus



2.1 Legal

Hay numerosas opciones gratuitas de antivirus que en realidad no hay razón para usar uno "pirata". Dado que un antivirus necesita de una actualización regular vía Internet para su correcto funcionamiento, si empleas un antivirus ilegal es posible que tarde o temprano seas detectado y el programa deje de funcionar o deje de actualizar sus definiciones. Algunos de los principales antivirus gratuitos son:

- Avast antivirus.

- Avira antivir.

- AVG.

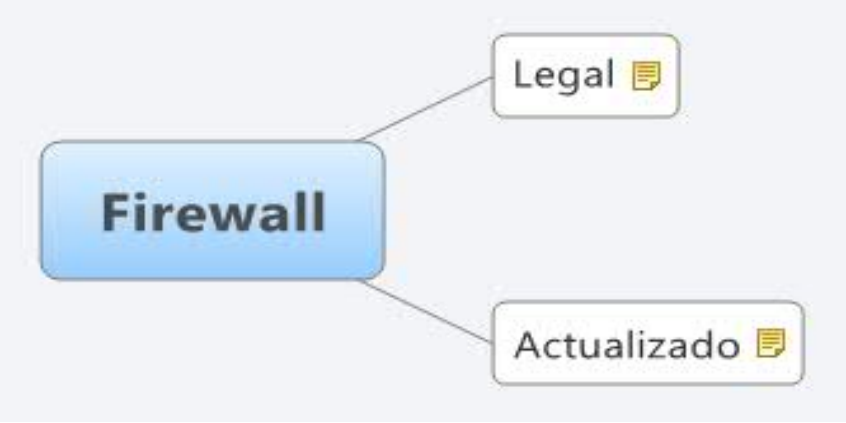
- ClamWin.

2.2 Actualizado

En materia de antivirus, no solamente hay que estar actualizado siempre a la última versión para que funcione correctamente, sino que es necesario haber descargado las últimas definiciones de virus. Las definiciones sirven para que el antivirus pueda detectar el virus y, si no puede eliminarlo, al menos que impida que se ponga en funcionamiento.

Algunos antivirus permiten descargarse sus definiciones aparte, de manera que puedas instalarlas más tarde en un computador que no cuente con conexión a Internet y contar así con el máximo de protección.

3. Firewall



3.1 Legal

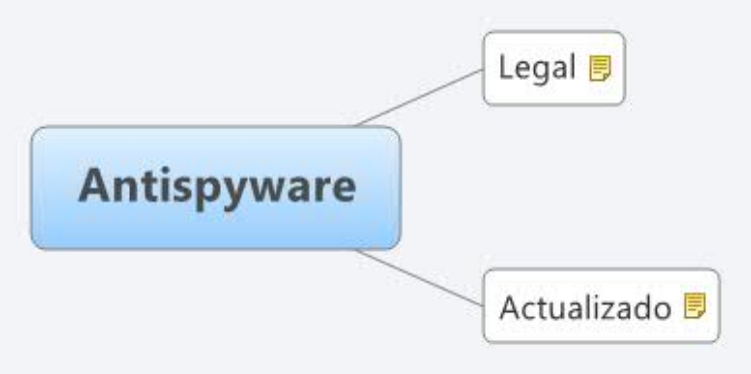
Un firewall nos protege de intrusiones en nuestra computadora, las cuales son más comunes de lo que nos pueda parecer. Estas intrusiones pueden limitarse al robo de datos (como el historial) o ir hasta el uso de nuestro equipo como un zombie que es usado para realizar ataques a webs.

Cualquier programa "pirata" de seguridad corre el riesgo de no poder actualizarse debidamente. Hay muchas alternativas gratuitas en materia de firewalls como para arriesgarse a usar uno ilegal. Entre ellas destaca el Comodo Firewall.

3.2 Actualizado

Las actualizaciones ofrecen soluciones a fallos de seguridad, detección de sitios web peligrosos y técnicas varias de infiltración en nuestro equipo. Además, en el caso de actualizaciones mayores, se incorporan nuevas funciones.

4. Antispyware



4.1 Legal

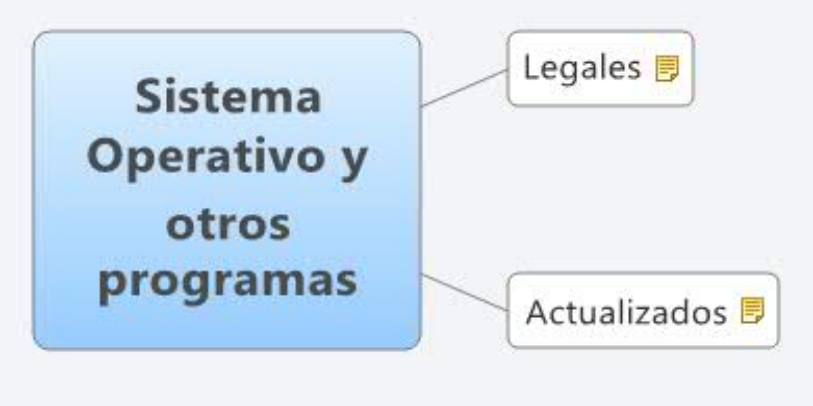
El antispyware detecta y elimina spyware instalado en nuestra computadora. El uso de un programa "pirata" de este tipo puede hacer que no se actualice regularmente, lo cual hará que nuestros datos corran el riesgo de ser robados.

Para evitar este programa, podemos utilizar muchas de las opciones gratuitas que existen, entre las que destaca Spybot Search & Destroy.

4.2 Actualizado

Es vital que un antispyware esté siempre actualizado para añadir las nuevas amenazas que van surgiendo. Hay que considerar que el spyware es una de las principales amenazas que nos podemos encontrar al navegar por la web debido a la facilidad con que se puede infiltrar en nuestro sistema sin que nos demos cuenta.

5. Sistema Operativo y otros programas



5.1 Legales

Todo sistema operativo recibe actualizaciones regulares no sólo para cubrir fallos de seguridad sino para mejorar su rendimiento. Igualmente sucede con muchos programas, por no decir todos (siempre y cuando aún continuen siendo desarrollados, que muchos que no).

Al utilizar programas "piratas" o ilegales se corre el riesgo de no poder actualizar cuando aparezca una nueva versión o de no recibir las actualizaciones menores (pero importantes) cuando salgan. Emplear software "pirata" hace nuestro sistema mucho más vulnerable a todo tipo de ataques.

5.2 Actualizados

Las actualizaciones de los sistemas operativos y los programas corrigen fallos de seguridad y problemas de rendimiento. En el caso de las actualizaciones mayores (como el paso de versión: de 2.0 a 3.0, por ejemplo) traen además nuevas funciones y características.

6. Complementos

En muchas ocasiones, se nos ofrecen complementos para programas o nuestro sistema operativo (emoticonos para el messenger, protectores de pantalla, etc). Hay que tener cuidado desde donde los descargamos, pues pueden ir acompañados de malware.

7. Correo electrónico

Consejos generales:

- Usa dos direcciones de correo electrónico, una con tus datos reales y otra con tus datos falsos. Emplea esta última cuando te sea necesario poner la dirección en un sitio del cual dudas de su fiabilidad.

- No dejes tu dirección en sitios visibles al público, como foros, comentarios en blogs, etc. Si lo haces, escríbela sustituyendo la arroba por una palabra. NO: usuario@servicio.com. SÍ: usuario_arroba_servicio_punto_com, por ejemplo entre otras variaciones.

- Nunca descargues archivos adjuntos de direcciones desconocidas. Así se contraen la mayoría de virus.

- No envíes NUNCA correos a multiples direcciones poniéndolas en el campo de la dirección ni en el de CC (Con Copia). Emplea el campo CCO (Con Copia Oculta). De esta manera, nadie podrá ver las direcciones de las otras personas y contribuirás a que se reciba menos Spam.

- El spam es el correo no deseado, ese que recibes con publicidad o con propuestas de negocios que te harán ganar dinero fácil y rápido. Nunca contestes a esos mensajes.

- De verdad, las cadenas no funcionan. No se te cumplirá el deseo si le envías ese texto a 50 personas más, ni siquiera a 5. Y si no lo envías, no te pasará nada.

8. Contraseñas

Consejos generales:

- Que sea fácil de recordar.

- Que sea larga (casi todos los servicios piden, como mínimo, 8 caracteres)

- Que alterne signos, números y letras en mayúsculas y minúsculas.

- Que no contenga información personal tuya que sea pública (es decir, que hayas publicado en Internet) o que sea fácil de obtener por métodos generalistas de ingenieria social (por ejemplo, una encuesta).

- Que sea rápida de escribir (esto no se comenta mucho, pero… ¿a qué prefieres no tardar mucho cada vez que entras en tu servicio web favorito?)

9. Descargas

Hay sitios que te piden que te descargues un archivo para poder acceder a su contenido. Desconfía de estos sitios y no te lo descargues. En la inmensa mayoría se trata de malware.

Si te pide que actualices algo de tu computadora, hazlo siempre yendo al sitio oficial de lo que te pida (por ejemplo, si te pide actualizar el Adobe Flash, ve a la página de Adobe). Si te sigue pidiendo que actualices después de haberlo hecho (o a pesar de estar seguro de que tienes la última versión), ignóralo y sal de ahí.

La mayoría de estos problemas suceden a la hora de ver vídeo o querer escuchar un audio. Ten cuidado con los sitios que visitas.

10. Mensajes no solicitados

- Si un sitio web te muestra un mensaje indicando que tienes un problema en tu computadora, o es falso, o se ha metido en tu equipo sin obtener tu permiso. Por lo tanto, no le hagas caso y sal de ahí.

- Lee todo cuadro de diálogo que aparezca en el navegador mientras navegas. Si no entiendes lo que pone, simplemente dale al botón "Cancelar". Nunca le des al botón "Aceptar" sin comprender que es lo que estás haciendo.

11. Ingeniería social

De Wikipedia:

En el campo de la seguridad informática, ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales (mejor conocidos como Script Kiddies o Defaces, aunque el termino correcto es cracker) para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil". En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, pretendiendo, por ejemplo, ser un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o memos falsos que solicitan respuestas e incluso las famosas "cadenas", llevando así a revelar información sensible, o a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, -por ejemplo proporcionando detalles financieros a un aparente funcionario de un banco- en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos.

Quizá el ataque más simple pero muy efectivo sea engañar a un usuario llevándolo a pensar que un administrador del sistema esta solicitando una contraseña para varios propósitos legítimos. Los usuarios de sistemas de Internet frecuentemente reciben mensajes que solicitan contraseñas o información de tarjeta de crédito, con el motivo de "crear una cuenta", "reactivar una configuración", u otra operación benigna; a este tipo de ataques se los llama phishing (pesca). Los usuarios de estos sistemas deberían ser advertidos temprana y frecuentemente para que no divulguen contraseñas u otra información sensible a personas que dicen ser administradores. En realidad, los administradores de sistemas informáticos raramente (o nunca) necesitan saber la contraseña de los usuarios para llevar a cabo sus tareas. Sin embargo incluso este tipo de ataque podría no ser necesario — en una encuesta realizada por la empresa Boixnet, el 90% de los empleados de oficina de la estación Waterloo de Londres reveló sus contraseñas a cambio de un bolígrafo barato.

Otro ejemplo contemporáneo de un ataque de ingeniería social es el uso de archivos adjuntos en e-mails, ofreciendo, por ejemplo, fotos "intimas" de alguna persona famosa o algún programa "gratis" (a menudo aparentemente provenientes de alguna persona conocida) pero que ejecutan código malicioso (por ejemplo, usar la máquina de la víctima para enviar cantidades masivas de spam). Ahora, luego de que los primeros e-mails maliciosos llevaron a los proveedores de software a deshabilitar la ejecución automática de archivos adjuntos, los usuarios deben activar esos archivos de forma explícita para que ocurra una acción maliciosa. Muchos usuarios, sin embargo, abren casi ciegamente cualquier archivo adjunto recibido, concretando de esta forma el ataque.