



Consejos de seguridad

- Asegurar el punto de acceso por ser un punto de control de las comunicaciones de todos los usuarios y por tanto críticos en las redes inalámbricas:
- Cambia la contraseña por defecto: todos los fabricantes ofrecen contraseñas por defecto de acceso a la administración del punto de acceso, al usar un fabricante la misma contraseña para todos sus equipos es fácil o posible que el observador la conozca.
- Aumentar la seguridad de los datos transmitidos: usar encriptación WEP o WPA, las redes inalámbricas basan su seguridad en la encriptación de los datos que viajan a través de aire. El método habitual es la encriptación WEP pero no podemos mantener WEP como única estrategia de seguridad ya que no es del todo seguro, existen aplicaciones para Linux o Windows que escaneando suficientes paquetes de información son capaces de obtener las claves WEP y permitir acceso de intrusos en nuestra red. Activa la encriptación de 128bits WEP mejor que la de 64bits. Algunos puntos de acceso más recientes soportan también encriptación WPA y WPA2, encriptación dinámica y más segura que WEP, si activas WPA en el punto de acceso tanto los accesorios como los dispositivos WLAN de tu red como tu sistema operativo debe de soportar.
- Ocultar tu red WIFI: cambia el SSID por defecto en lugar de mi AP o Apmanolo o el nombre de la empresa es preferible coger algo menos atractivo como wroken, down o desconectado, si no llamamos la atención del observador hay menos posibilidades de que este intente entrar en nuestra red.
- Desactiva también el broadcasting SSID o identificador de la red inalámbrica. El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red wifi identifiquen automáticamente el nombre y los datos de la red inalámbrica evitando así la tarea de configuración manual. Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.
- Evitar que se conecten:

- Activa el filtrado de direcciones mac: para activar el filtrado mac dejaras que solo los dispositivos con las direcciones mac especificadas se conecten a tu red wifi. Por un lado es posible conocer las direcciones mac de los equipos que se conectan a la red con tan solo escuchar con el programa adecuado ya que las direcciones mac se transmiten en abierto sin encriptar entre el punto de acceso y el equipo, además aunque en teoría las direcciones mac son únicas a cada dispositivo de red y no pueden modificarse hay comando o programas que permiten simular temporalmente por software una nueva dirección mac para una tarjeta de red.
- Establece el número máximo de dispositivos.
- Desactiva DHCP en el router o en el punto de acceso en la configuración de los dispositivos o accesorios WIFI, tendrás que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y los DNS. Si el observador conoce el rango de IP que usamos en nuestra red no habremos conseguido nada con este punto.
- Desconecta el AP cuando no lo uses: el AP almacena la configuración y no necesitaras introducirla de nuevo cuando lo conectes.

Cambia las claves regularmente: puede ser necesario entre 1 y 4 GB de datos para romper una clave WEP dependiendo de la complejidad de las claves de manera que cuando llegue a este caudal de información transmitida es recomendable cambiar las claves.

Formas de Protegernos

Virus Informático

Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus son programas que se replican y ejecutan por sí mismos; tienen la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) efectos nocivos y a veces irreparables.

Daños: Pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos, son la pérdida de información, horas de parada productiva, tiempo de reinstalación, etc.

Formas de contagio: Las formas de contagio más usuales son las siguientes: Una es por causa de la red y la otra forma es ejecutando un archivo ya infectado.

Forma de combatirlos

Un buen ANTIVIRUS los cuales son los encargados de encontrar estos archivos infectados y eliminarlos de tu computador (solo se encargan de eliminar el archivo infectado pero si es que esta ya había causado daños dentro de su computador, el antivirus en ningún caso podrá o reparar dichos archivos), como por ejemplo: avast!, nod32, kaspersky, bitdefender, etc.

Gusanos (Worms)

Un gusano es un virus informático que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. Los gusanos siempre dañan la red (aunque sea simplemente consumiendo ancho de banda).

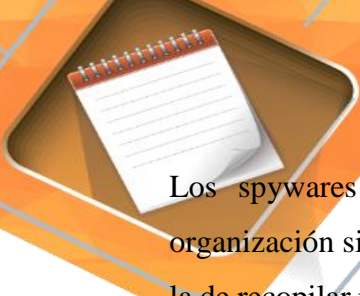
Es algo usual detectar la presencia de gusanos en un sistema cuando, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

Daños: Un gusano tiene por finalidad consumir los recursos de un computador y hacer que el consumo de recursos sea tal de que hasta las tareas más ordinarias no puedan ejecutarse.

Formas de combatirlos

Un ANTIVIRUS actualizado como los ya mencionados anteriormente. A pesar de que un gusano puede causar una molestia enorme, un antivirus actualizado es capaz de mantenerte casi en la totalidad de ellos a salvo (en estos últimos tiempos se han creado unos gusanos más avanzados que han llegado al nivel de transmitirse a través de e-mails).

Spywares (Programas espías)



Los spywares son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, con el objetivo de obtener información importante. Dado que el spyware usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual, puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otra(s) conectada(s) a Internet.

Daños: Robo de información, consumen ancho de banda y lo más molesto que hacen (que a la vez es peligroso) es apagar tu computador sin previo aviso

Formas de combatirlos

En la algunos casos los antivirus no son capaces de encontrar los spywares por eso la manera más eficaz es con un anti-spyware que son los encargados de eliminar estos problemas de una manera eficaz (además estos también eliminan los cookies). Algunos ejemplos de softwares anti-spywares son: spyware-serch & destroy, spyware doctor, SUPERAntispyware, etc.


Caballos de Troya (Troyanos)

Se denomina troyano a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.

Daños

Infectar archivos, subir y bajar archivos infecciosos a la red, ser una puerta de enlace para la descarga de virus, funcionar de controlador remoto (que otra persona ajena haga uso y desastres dentro de tu computador [hackers y lamers]), alteraciones en el hardware, robar información de tu computador, auto ejecutar virus informáticos, reiniciar o apagar el equipo sin previo aviso, etc. En pocas palabras, un troyano tiene las facultades de hacer una destrucción total de un computador.

Formas de combatirlos



Un buen antivirus actualizado podría ser una buena solución aunque es mejor borrarlos manualmente del registro para así evitar que este se vuelva a crear. Generalmente los troyanos se alojan en el registro en una inofensiva carpeta así que para acabar con él es ir a inicio/ejecutar/regedit con esto se entrara al registro donde se almacena todas las configuraciones y cambios de registro que hay dentro de tu computador (hay que tener conocimientos informáticos)

***Soluciones en caso de infección**

- Detecta la Infección
- Anote el nombre del virus y de los archivos infectados, pero no seleccione la opción Eliminar la infección
- Comprobar de que no queda ninguna infección
- Actualizar el antivirus

Actualice su antivirus residente (o instale uno si todavía no lo ha hecho).