Capítulo 10

Seguridad

hat
ideweb
ork
email

CAPÍTULO 10 - Seguridad en Internet

Los Virus

Los virus informáticos son programas que se instalan de forma inadvertida en los ordenadores, realizan su función destructiva y pueden propagarse hacia otros ordenadores.

Las vías de propagación son diversas y han ido evolucionando a lo largo del tiempo. Hace unos años, cuando no existía Internet, se propagaban preferentemente a través de los disquetes. Luego empezaron a utilizar como vía de expansión los programas que se descargaban por Internet.

Los medios más utilizados de propagación son el email (correo por Internet) y las páginas Web. Utilizar el correo como medio de dispersión tiene varias ventajas desde el punto de vista de los virus. En un medio muy rápido y utilizado por muchas personas, un virus puede replicarse millones de veces en pocos días de la siguiente forma.

El virus llega por correo a un ordenador y se autoenvía a todas las direcciones de correo que figuren en la Libreta de Direcciones. Al llegar a otro ordenador se vuelve a autoenviar a todas las direcciones que figuren en él, y así sucesivamente.

Los virus que utilizan las páginas Web e Internet también son capaces de reproducirse muy rápidamente puesto que una página puede ser visitada por miles de personas al día.

El ciclo de vida de un virus podría ser este, entra en nuestro ordenador, es decir, nos infecta, se ejecuta y causa, normalmente, daños, luego intenta copiarse en otros ordenadores, es decir propagarse. Cuando es detectado por algún programa antivirus o por el usuario es eliminado y muere. Vamos a ver todo esto con más detalle.

Cómo se realiza la Infección

Para que nuestro ordenador se infecte o contagie con un virus, el código del virus tiene que grabarse en nuestro ordenador, la forma más sencilla de hacer esto para un virus es cuando copiamos archivos, ya que sólo tiene que ocultarse dentro del archivo que estamos copiando.

Si sólo leemos información no podremos infectarnos, por ejemplo, si leemos el contenido de un CD o visitamos una página de la web no hay peligro de infección. Esto es la norma general, pero hay excepciones, como veremos más adelante, ya que a veces ocurre que estamos grabando cosas en nuestro ordenador sin darnos cuenta de ello.

Una vez el archivo del virus está en nuestro ordenador tiene que ejecutarse para poder realizar sus funciones. El hecho de tener un archivo grabado en el disco duro no quiere decir que ese virus haya hecho todo lo que tiene que hacer, puede que todavía no se haya ejecutado. Aunque lo más normal es que nada más entrar en el ordenador el archivo se ejecute. Hay varias formas de ejecutarse, por ejemplo, lo podemos ejecutar nosotros mismos sin darnos cuenta al abrir un archivo adjunto del correo. Otra forma de autoejecutarse es alterar la configuración del ordenador para que se ejecute cada vez que arrancamos el ordenador. Así pues, cada vez que copiamos algo en nuestro ordenador podemos estar copiando también un virus.
Las vías de infección más comunes son:

1- El correo electrónico.
2- Bajarse archivos de Internet por download.
3- Bajarse archivos de Internet por ftp.
4- Copiar disquetes, CD, etc.
5- Visitar páginas web.
6- Uso de grupos de discusión.
7- Uso de redes.
8- Uso de redes P2P.

1- El correo electrónico

Es el método de infección más importante en la actualidad. Permite a los virus expandirse a gran velocidad ya que se envían millones de correos cada día. Algunos virus sólo se activan si abrimos los ficheros adjuntos que acompañan al mensaje.

Otros virus se activan simplemente al abrir el correo y leer el mensaje. Si tenemos activada la vista previa en nuestro programa de correo implica que se leen todos los mensajes para mostrar el asunto y el remitente, por esto aunque nosotros no abramos el mensaje, el programa de correo sí lo abre y por lo tanto podemos contagiamos. Más adelante, en el punto Precauciones puedes ver cómo desactivar la vista previa.
Leer el correo, en muchos casos, es una acción que hace que se grabe información en nuestro ordenador. Ya que los mensajes son descargados del servidor de correo y grabados en nuestro disco duro.

2- Bajarse archivos de Internet por download

Hay muchas páginas web que dan la posibilidad de descargarse archivos haciendo clic en un enlace, se abre un cuadro de diálogo para preguntarnos en qué carpeta de nuestro disco duro queremos dejar el archivo y comienza la descarga. Si el archivo que descargamos está infectado puede infectar nuestro ordenador.

3- Bajarse archivos de Internet por ftp

Esta es otra forma de descargarse archivos por la red. Para ello se utilizan programas de ftp como Cute-FTP o SmartFTP, estos programas permiten conectar con un servidor y copiar archivos del servidor a nuestro ordenador y si estamos autorizados desde nuestro ordenador al servidor.

4- Copiar disquetes, CD, etc. (Dispositivos de almacenamiento)

Hasta hace pocos años este era el método más utilizado por los virus para expandirse, hoy en día se copian menos archivos utilizando discos ya que es más fácil enviarlos por Internet. Últimamente, con el uso masivo de dispositivos de almacenamientos tipo pendrives, etc han aparecido algunos programitas molestos que no llegan a ser virus fatales, pero si harán que funcionen lentos o hasta no permitan ser reconocidos por la computadora.

5- Visitar páginas web.

Normalmente las páginas web contienen texto, gráficos, sonido, animaciones y vídeos. El navegador sólo se leen estos elementos y se visualizan en la pantalla, por lo tanto las páginas web no pueden infectarnos ya que no suelen contener programas que se ejecuten en nuestro ordenador.

Sin embargo algunas páginas web pueden grabar información en nuestro ordenador por medio de los controles ActiveX y Applets Java sin que seamos conscientes de ello. Este es un medio de infección muy peligroso y que cada vez se utiliza más, sobre todo para propagar programas espía.

Normalmente, para que una página web pueda infectar a sus visitantes ha de ser el propio dueño o webmaster de dicha página el que instale los virus con intención de propagarlos, por lo tanto puedes navegar tranquilamente por todas las páginas serias de la red. Casi el 100% de los servidores tienen antivirus que evitan la posibilidad de enviar virus a través de sus páginas web.

Los fallos en construcción de los navegadores también están involucrados en este sentido. Muchas veces al programar el funcionamiento de los navegadores se dejan huecos o agujeros con debilidades que personas malintencionadas utilizan en nuestra contra. De hecho, en Septiembre del 2006 se encontró un falló en Internet Explorer que permitía instalar cualquier cosa en un navegador simplemente por haber visitado una web.

En este último caso, la interacción del usuario en la infección es casi nula, normalmente (y en otros casos) nos infectamos por descargar un archivo, ejecutar un programa o hacer clic en determinado enlace. Si se aprovechan este tipo de fallos el resultado puede ser caótico pues nada más visitar la página nuestro equipo estaría a merced de cualquiera.

De todas formas, como hemos dicho antes, se trata solamente de hechos aislados que se solucionan parcheando (arreglando) el programa navegador. Y aun así, los servidores y páginas webs de confianza no suelen tener estos tipos de problemas.

La única solución es ser precavido y visitar sólo sitios que consideremos seguros.

6- Uso de grupos de discusión, chats, IRC.

En los grupos de discusión se intercambian mensajes y en ocasiones también archivos adjuntos, de forma similar al correo. Aunque los grupos de discusión utilizan un sistema de transmisión distinto al correo, es posible que si abrimos alguno de estos adjuntos nos podamos contagiar.

Potencialmente cualquier medio de transmitir archivos es susceptible de usarse para enviar un virus.

7- Uso de redes.

Podemos contagiarnos al utilizar redes globales (Internet) o redes locales.
Hasta ahora el caso más claro de infección a través de Internet ha sido el virus Sasser que contagia ordenadores por el simple hecho de conectarse a Internet, sin que el usuario visitase una página web determinada o se descargase un archivo.

Cuando utilizamos una red local estamos compartiendo recursos con los demás ordenadores de la red, si alguno de los ordenadores de la red está autorizado a escribir en nuestro disco duro podría transferirnos un virus.

8- Uso de redes P2P.

Las redes P2P (eMule, eDonkey, bitTorrent, ...) están pensadas para el intercambio de archivos y son utilizadas por millones de personas en todo el mundo, por lo tanto son el lugar ideal para colocar archivos con virus mezclados entre los archivos sanos. Hay que decir que estas redes toman medidas para evitar la presencia de virus y en cuanto detectan alguno lo eliminan o avisan a sus usuarios.

Y volvemos a repetir: potencialmente cualquier medio de transmitir archivos es susceptible de usarse para enviar un virus.

Sólo por el hecho de participar en un chat o grupo de discusión, enviando y recibiendo mensajes no significa que tengas que contagiarte.

Propagación

La rapidez de propagación es el aspecto que determina que un virus tenga más o menos éxito. Los creadores de virus no paran de buscar nuevos métodos de propagación más rápidos y difíciles de detectar.
La propagación incluye varios aspectos como el punto de entrada en el ordenador o infección, el lugar donde esconder el archivo y la forma de activarse. Si el punto de entrada es poco común se podrán infectar pocos ordenadores. Si el archivo con el virus no se esconde bien será detectado rápidamente y no podrá propagarse. Si no se activa antes de ser detectado tampoco se expandirá mucho.

Los lugares donde se pueden esconder los virus y su forma de activarse son:

- Archivos adjuntos en los correos. Al abrir el archivo adjunto el virus se activa.
- Dentro del código de algunos archivos, como las macros de los documentos word o excel. Estos documentos pueden contener macros que realizan funciones adicionales en el documento, pero en el fondo una macro no es más que un programa que viaja con el documento. Al abrir el documento se ejecuta la macro y el virus se puede activar.
- En la memoria del ordenador. Desde la memoria puede ejecutarse en cualquier momento y copiarse a otro archivo.
- En archivos ejecutables. Los archivos ejecutables más comunes tienen extensión .exe o .com, y son los archivos que contienen programas. Estos archivos contienen código que se ejecuta al abrirlos.
- En los sectores de arranque de los discos. Cada vez que se lee un disco se lee el sector de arranque del disco, es pues un buen lugar para esconder el código del virus.
- En páginas web no confiables. Muchas empresas de pornografía instalan programas en nuestras computadoras para mandar publicidad o mostrar anuncios sin ningún tipo de filtro.

Daños y efectos causados

El primer fin de un virus es propagarse y el segundo fin exhibirse, mostrar que existe. Si un virus no se exhibe será más difícil de detectar.

- La exhibición puede ser destructiva o festiva.
- La destructiva puede tener varios grados, desde inutilizar algún programa o borrar un fichero concreto hasta borrar el disco duro o bloquear el sistema operativo.
- La exhibición festiva puede consistir en mostrar algún mensaje en la pantalla o hacer que un dibujo aparezca moviéndose por la pantalla o emitir algún sonido, etc.

Hay algunos creadores de virus que sólo quieren mostrar su habilidad y demostrar que son capaces de encontrar las "puertas abiertas" o debilidades de los programas comerciales. Los ordenadores casi nunca se equivocan, pero los programas que los haces funcionar no son infalibles. Un programa puede contener millones de líneas de código, es posible que algún detalle se haya escapado a sus programadores, la misión del creador de virus es encontrar esos detalles que permiten que el programa funcione de una forma no prevista en determinadas situaciones.

Los creadores de virus suelen tener afán de notoriedad, si su virus realiza una acción destructiva será más conocido y temido que si no hace nada dañino.

En algunos casos y países las leyes no están adaptadas a las nuevas tecnologías por lo que los delitos informáticos pueden no estar tipificados, además un virus puede ser creado en un país con un vacío legal y expandirse desde ahí por todo el mundo.

Detección

La forma más evidente y penosa de enterarnos es como consecuencia de los daños producidos por el virus, y que acabamos de ver en el punto anterior.

Sin embargo hay algunos síntomas que nos pueden alertar de la presencia de un virus. Hay síntomas dudosos que pueden ser por un virus o por otras causas y que deben dar lugar a una investigación más profunda. Hay otros síntomas claros de que estamos infectados y que obligan a una actuación urgente.

Síntomas dudosos:
- la computadora funciona muy lenta.
- disminuye la memoria disponible.
- el ordenador se apaga, bloquea o cuelga frecuentemente.
- hay programas que no funcionan o funcionan mal a partir de un momento dado.

Síntomas claros.
- queda menos espacio libre en el disco duro sin que nosotros grabemos archivos.
- desaparecen archivos del ordenador.
- aparecen mensajes o gráficos extraños en la pantalla.
- al pulsar una tecla o un acento no funciona correctamente.
- algunos archivos cambian de nombre o de extensión.
- el lector de CD se abre y cierra solo.

La presencia de algunos de estos síntomas implica que ya se han producido daños, como en el caso de observar que han desaparecido archivos, pero siempre es bueno darse cuenta cuanto antes.

En resumen, cualquier acción extraña que no podamos asociar a ninguna otra causa puede ser causada por un virus.

La mejor forma conocida de detectar un virus para los usuarios sin conocimientos de informática es ejecutar un programa antivirus.

Tipos de virus

Los virus se pueden clasificar según diferentes criterios. Vamos a ver los más usuales.

Gusanos.

Estos virus no se copian dentro del código de otros ficheros sino que se copian ellos mismos. Los gusanos más frecuentes son los que se copian utilizando la libreta de direcciones de Microsoft Outlook. Se envían a sí mismos como ficheros adjuntos. También existen gusanos que se propagan a través de los canales de IRC.

Para activarse pueden modificar el registro de Windows de forma que cada vez que se ejecute un archivo con extensión .EXE el virus se activará.

Ejemplos de este tipo de virus son el virus W32/SIRCAM y el virus I_LOVE_YOU

Si recibes un correo que tenga el asunto TE ENVIO ESTA DIVERTIDA HISTORIA, puede ser el virus I_LOVE_YOU

Residentes

Estos virus permanecen en la memoria RAM esperando a que se cumplan determinadas condiciones de activación para propagarse y causar daños. Al apagarse el ordenador desaparecen de la memoria, pero son capaces de modificar el registro de Windows para volver a colocarse en memoria cuando se enciende el ordenador.

Ejemplos de este tipo de virus son Barrotes y Viernes13. Este último está programado para borrar cualquier programa que se ejecute el día 13, si cae en viernes.

Troyanos.

Este tipo de virus se camufla dentro de un programa que parece inofensivo e interesante, para que el usuario lo ejecute y así llevar a cabo el fin para el que fueron programados. En ocasiones lo que pretenden es sacar al exterior información de nuestro ordenador, como podrían ser contraseñas y otros tipos de datos que pudieran ser valiosos. Por ejemplo, el troyano Crack2000 se distribuye junto con un programa que dice llevar los números de serie de aplicaciones comerciales, una vez instalado hace que se envíe por FTP la información grabada en el disco duro.

Macros.

Estos virus están dentro del código de las macros de programas como Excel, Word o CorelDraw. Por ejemplo el virus Melissa es una macro de Word97.

Ejecutables.

Gran parte de los virus forman parte del código de ficheros ejecutables de extensión .EXE y .COM. Podríamos decir que es el tipo de virus más común. Estos virus se ejecutan cuando lo hace el fichero en el que se encuentran y utilizan diversos medios para propagarse. Los virus incluidos en ficheros ejecutables no son un tipo puro de virus sino que pueden tener además alguna de las características de otros tipos de virus. Por ejemplo hay virus ejecutables que se propagan por el correo como los virus tipo gusano.

Malware

Todos estos sistemas de propagación que hemos visto no se aprovechan únicamente para infectarnos con Virus, sino que también se utilizan para instalar en nuestros ordenadores programas que maliciosamente interfieren con la información que enviamos o poseemos.

Este tipo de programas se llama Malware. El Malware está diseñado para insertar y distribuir virus, troyanos, o pequeños programas que recogerán información sobre nuestro ordenador y lo utilizará con malas intenciones. El Malware, también, suele ir incrustado o añadido en programas gratuitos de dudosa procedencia que podemos encontrar por Internet. Ten cuidado con ellos porque pueden llegar a ser igual de desastrosos que los virus.

Algunos sitios pornográficos o que dicen contener claves para romper la seguridad de programas comerciales obligan a instalar al usuario este tipo de programas camuflados bajo barras de navegación u otro tipo de elementos que instalarán este tipo de programasen nuestra computadora.

El Malware también se dedica a instalar Spyware en nuestra computadora, un programa espía o spyware recopila información sobre nosotros y lo envía normalmente a empresas de publicidad. De esta forma podemos empezar a recibir SPAM sin haberlo pedido expresamente.

Si a pesar de todo el Spyware se instala en tu ordenador, existen herramientas anti-spyware (como Spybot) que recorren tu disco en busca de programas instalados que pudieran ser maliciosos (de ahí también el término Malware) y peligrosos para tu privacidad.

SPAM

SPAM es la palabra que se utiliza para calificar el correo no solicitado con fines comerciales o publicitarios enviado por Internet.

Los usuarios que los reciben pagan por el envío de su propio bolsillo, el Spam es una publicidad cuyo coste recae en quien la recibe aunque no quiera hacerlo. Cualquiera que tenga un servicio de acceso a Internet que pague por tiempo o por tráfico, lee o recibe mensajes, como si dijéramos, con el contador en marcha, los que tienen tarifas planas funcionan peor.

Todas las conexiones van más lentas debido a las ingentes cantidades de tráfico que genera el Spam, leer los mensajes Spam incrementa su factura de teléfono, le ocupa tiempo, espacio en su buzón y le puede hacer perder información que se quiere recibir. Además, a los Proveedores de Servicios de Internet (ISPs), Operadores de Telecomunicaciones y de servicios Online les cuesta dinero transmitir y gestionar los millones de mensajes que genera el Correo Basura, y esos costes se transmiten directamente a los suscriptores de dichos servicios.

Aunque las acciones a tomar realmente tienen que ver más con la personalidad de quien recibe el mensaje, el tiempo invertido en combatirlo es completamente perdido, por lo tanto se sugiere que simplemente se borre el mensaje del buzón y suponga que no se recibió. Muchos de estos son distinguibles a simple vista porque incluyen o el signo del dólar, o valores en el encabezado. Otros incluyen las palabras GRATIS o FREE igualmente.

Se recomienda entonces, no tener en cuenta estos mensajes y hacer lo que hacen el 55% de los usuarios de la red: borrarlos. En caso de que el volumen de mensajes sea muy alto (10 o más al día) se sugiere tomar otro tipo de medidas que pueden ir desde la solicitud de ser borrados de las listas hasta la difusión de la información del infractor.

Hay que tener presente que los autores del Spam cuentan con herramientas muy sofisticadas para recolectar direcciones E-mail válidas, entre ellas podemos citar los programas webspiders que permiten rastrear páginas web, news y otros recursos de Internet.

Por lo tanto:

Sólo hay que dar la dirección E-mail a amigos y conocidos.

No publicar la dirección E-mail en las News o en páginas Web.

No rellenar formularios en los que se soliciten datos personales.

Nunca hay que contestar a un mensaje de Spam ya que en muchos casos la dirección del remitente será falsa y devuelven el mensaje y si no es falsa sirve a la empresa de publicidad para saber que la dirección E-mail es correcta.

Precauciones

Hoy en día los virus se propagan de múltiples formas, sobre todo el envío de virus por correo se ha convertido en algo común y hay que tomar precauciones, cuantas más mejor.

- No hay que abrir correos de desconocidos o que nos merezcan poca confianza.
- No abrir archivos adjuntos si no se tiene la certeza de su contenido incluso si proviene de una dirección "amiga".
- También es conveniente fijarse en el texto del Asunto, si es un texto sin un significado claro puede ser un síntoma de que el correo contiene un virus ya que algunos virus generan el asunto juntando varias palabras al azar.
- Desactivar la opción de "Vista previa" de algunos programas de correo, como por ejemplo el Outlook Express. Así evitamos que siempre se lea el mensaje para poder mostrar la Vista Previa.

- Es más seguro leer el correo utilizando el webmail o correo a través de la web, como Hotmail, Yahoo, Hispavista, etc. Esto es así por dos razones fundamentalmente. La primera es que al leer por la web podemos hacer que no se grabe nada en nuestro disco duro desactivando la copia de páginas en caché. Ojo que si abrimos los archivos adjuntos sí se pueden grabar archivos en nuestro ordenador. La segunda razón es porque los servidores de correo web suelen tener buenos filtros antivirus.
- Hay que tener mucho cuidado con los archivos y programas que nos bajamos de Internet, especialmente de sitios sospechosos.
- Los programas antivirus pueden trabajar de dos formas básicas. De forma permanente y bajo petición.

De forma permanente quiere decir que el antivirus se instala de forma residente en memoria y busca virus en todos los archivos que se abren o descargan de Internet. Es la forma más segura de protegerse de los virus. Tiene el pequeño inconveniente que consume memoria RAM y en algunas ocasiones puede interferir el funcionamiento de algunos programas.

De forma puntual o bajo petición, podemos tener el antivirus desactivado y activarlo sólo cuando consideremos que hay peligro de contagio, por ejemplo cuando descargamos archivos de Internet, copiamos un disquete o instalamos un programa nuevo.

Es conveniente tener activado el antivirus de forma permanente.

- Hay que actualizar frecuentemente el programa antivirus, ya que cada poco tiempo aparecen virus nuevos que un antivirus no puede detectar hasta que no es actualizado.
- Si sólo utilizamos software legal es más difícil que nos contagiemos.
- Por muchas precauciones que tomemos no está garantizado al 100% que no nos podamos infectar, por lo tanto conviene realizar copias de seguridad de nuestros datos en CD u otros medios. Si se estropea el ordenador por otras causas ajenas a los virus también agradeceremos tener una copia de seguridad.

Todas las precauciones se resumen en tres, utilizar un buen programa antivirus actualizado, no grabar archivos sin garantía y no abrir correos de remitente desconocido.

Eliminación de Virus

Lo más importante en este tema de los virus es tomar las medidas preventivas para no infectarse. Una vez infectados, para un usuario sin conocimientos de informática, será un poco complicado eliminar el virus de su ordenador. Lo más sencillo es recurrir a un programa antivirus.

Cada tipo de virus se elimina de una determinada forma, y cada virus concreto infecta unos archivos concretos, no hay una forma general que sirva para eliminar los virus de un tipo dado. Los programas antivirus suelen ser eficaces en la tarea de eliminar un virus de un ordenador.

También puedes visitar la página web de los fabricantes de antivirus, algunos de ellos dan información para la desinfección manual de forma gratuita como por ejemplo, Panda. Realmente no es muy complicado eliminar un virus a partir de las instrucciones proporcionadas por las páginas web de los fabricantes de antivirus, el problema es que sin nos equivocamos podemos causar algunos desbarajustes en el sistema operativo ya que para eliminar un virus a mano hay que modificar, en muchas ocasiones, archivos del sistema operativo y del registro de Windows.

En algunas ocasiones borrar el fichero que contiene el virus suele ser suficiente para eliminarlo, pero en otros casos no es tan fácil ya que el código del virus está dentro de archivos que contienen programas necesarios para que funcionen el ordenador y no se pueden borrar.

Otras veces, además de borrar archivos también hay que borrar elementos del registro de Windows que permiten que el virus se active.

Un buen antivirus debe ser capaz de detectar los virus antes de que infecten el ordenador, avisándonos para que no continuemos con la tarea que está provocando la infección, normalmente la descarga o copia de un archivo o la lectura de un correo electrónico.

Cuantos más virus sea capaz de detectar mejor será el antivirus, pero lo más importante es que ante la aparición de un nuevo virus sea capaz de ofrecer una solución en un corto periodo de tiempo y que además la ponga a disposición de sus clientes a través de una actualización por Internet, lo que asegura la mayor rapidez posible en la protección de los usuarios del programa antivirus.

Para disponer de estos servicios hay que estar registrado como comprador del programa antivirus.

Aunque cuando se producen ataques masivos de virus peligrosos algunas compañías suelen proporcionar herramientas de desinfección de forma gratuita.

Antivirus más conocidos

- Panda,
- MacAffee,
- Symantec,
- AVG
- Kaspersky
- Nod32
- Prevx

Cortafuegos (Firewall)

Un cortafuegos o firewall (en Inglés) es un sistema hardware y/o software que permite controlar quién entra y quién sale del ordenador. Es como un filtro que impide que se puedan colar intrusos en nuestra computadora. Hoy en día existe una nueva amenaza, es la intrusión en los ordenadores conectados a redes sin que el usuario se descargue nada ni visite ninguna web, simplemente con estar conectado es suficiente para que alguien pueda entrar e instalar programas espía (spyware) o programas fraudes (phishing) o llegar a controlar totalmente el ordenador. Todo esto puede estar sucediendo en tu ordenador sin que te enteres, hasta hace poco, contra estos ataques, los programas antivirus convencionales no solían protegernos, ya que hace falta un cortafuegos. Actualmente, los cortafuegos suelen venir incluidos con la mayoría de antivirus de pago y son un complemento más del programa, aunque a veces no suelen estar incluidos en las versiones básicas. Las últimas versiones de Windows XP (a partir del ServicePack2) también incluyen uno. Para configurar un cortafuegos hay que definir unas reglas que determinan quien puede y quien no puede acceder al ordenador. Si tienes una red local instalada deberás redefinir los parámetros de tu cortafuegos para que los ordenadores que forman la red local se puedan comunicar entre sí porque si no, tu cortafuego impedirá el acceso a tu ordenador por parte de los demás ordenadores de la red.

Centro de Seguridad de Windows

El centro de seguridad de Windows es el encargado de supervisar el estado del quipo en cuanto a protección se refiere. Puedes acceder a él haciendo clic en Inicio Panel de control y seleccionando Centro de seguridad. En él hay tres puntos importantes: el Firewall o cortafuegos, las Actualizaciones automáticas y la Protección antivirus.

Aquí puedes ver el estado de cada una de estas secciones.

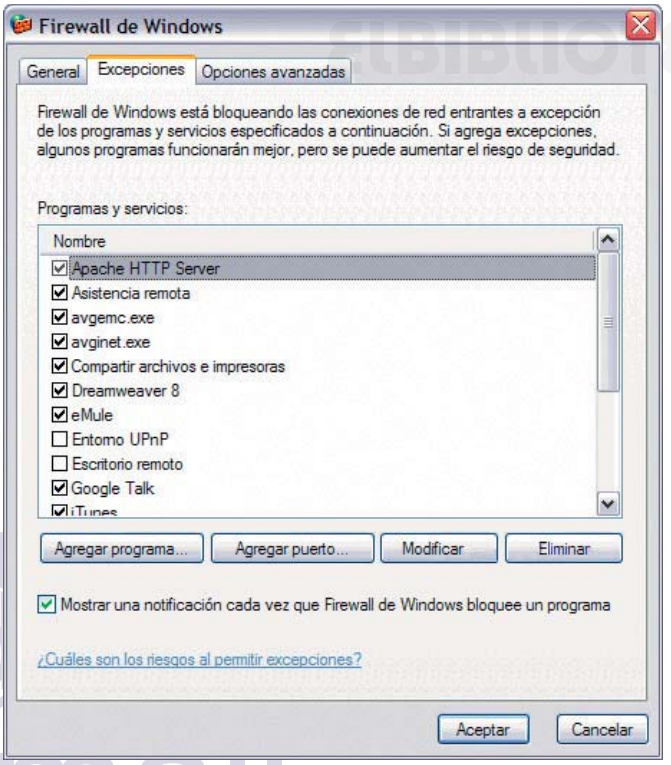
Desde los enlaces que se encuentran al pie de la ventana podrás acceder a su configuración.

Haciendo clic en Firewall de Windows podrás ver un cuadro de diálogo parecido al que ves en la imagen a la derecha. (Seleccionamos la pestaña Excepciones para la configuración avanzada).

Desde la pestaña Excepciones podemos elegir qué programas queremos que tengan acceso a Internet. De esta forma sólo aquellos que nosotros queramos podrán comunicarse con el exterior.

Ahora imagina que se instala un troyano en tu computador. Cuando se ejecute intentará ponerse en contacto con el exterior para enviar información.

Si el troyano no está en esta lista no será capaz de acceder a la red.

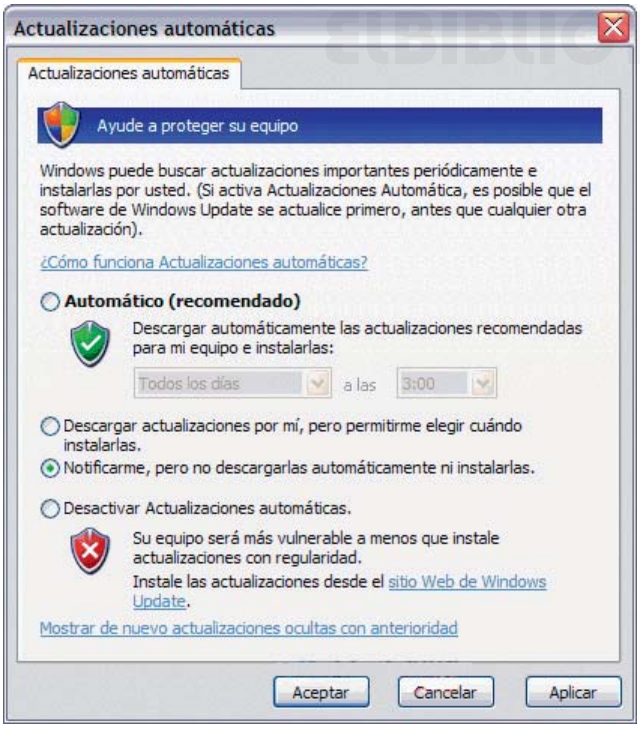


Haciendo clic en el enlace Actualizaciones automáticas (en la ventana del Centro de seguridad) abrirás el cuadro de diálogo que ves a tu derecha. Desde aquí podemos controlar cómo se producirá el flujo de actualizaciones en nuestro ordenador.

Otra de las causas de la infección son los fallos o agujeros en los programas que utilizamos, entre ellos el sistema operativo (Windows), los programas de navegación (Internet Explorer) o de reproducción de archivos (Windows Media Player).

Ambos productos pertenecen a Microsoft, por lo que se ha creado está característica. A medida que se van descubriendo nuevos puntos flacos en los programas, se van liberando parches o soluciones. Utilizando las Actualizaciones automáticas podemos asegurarnos de que nuestra copia de Windows, y todos los programas vinculados a él, funcionan correctamente y están protegidos de ataques externos.

Utiliza las opciones que ves a tu derecha para configurar el modo en el que estas actualizaciones se descargarán y se instalarán.



Finalmente, si observas el Centro de seguridad verás que hay una sección dedicada al antivirus. Windows no puede acceder a la configuración del programa antivirus que tengas instalado en tu PC, pero sí puede avisarte sobre su estado.

Si en algún momento tu antivirus se queda desactualizado, es decir, su base de datos sobre virus es demasiado antigua, Windows te avisará a través del Centro de seguridad.

Si no quieres instalarte un programa antivirus, y tampoco quieres que Windows te avise de que tu equipo corre peligro puedes desactivar estos avisos seleccionando Protección antivirus y haciendo clic en el botón Recomendaciones. Se abrirá el cuadro de diálogo que ves a tu derecha, marca la casilla Tengo un programa antivirus que yo supervisaré.

De todas formas, aunque tengas instalado un antivirus, es posible que Windows no lo detecte. Sigue estos mismos pasos para evitar el aviso continuado de que tu equipo está en riesgo.

Phising

Por último veremos un método malicioso que pretende robarnos información de nuestras cuentas bancarias: el Phishing. El Phishing se está poniendo muy de moda últimamente, millones de usuarios reciben a diario correos de entidades bancarias pidiendo que se proporcionen claves o números de cuenta a los usuarios para realizar una serie de comprobaciones. Pues bien, diremos desde un principio que estos correos son FALSOS.

En ningún momento tu entidad bancaria, tu sitio de micropagos (PayPal) o cualquier empresa te requerirá datos sobre tus cuentas bancarias por e-mail. Lo que reproducen estos correos son avisos de ciertas entidades imitando su diseño. Normalmente aparecen enlaces a páginas que a primera vista parecen ser de tu propio banco, pero si miramos con más atención nos damos cuenta de que son servidores que no tienen nada que ver con él. Estos enlaces dirigen en realidad a páginas creadas por personas malintencionadas que pretenden que les proporcionemos la información suficiente como para vaciarnos la cuenta corriente.

Las medidas que deberemos tomar cuando tratamos con entidades de este tipo son las siguientes:

- Como hemos dicho antes, tu entidad bancaria NUNCA te pedirá por correo información de este tipo.
- Siempre que accedas a tu banco hazlo escribiendo tú mismo la dirección en el navegador, no utilices enlaces.
- Si haces clic en un enlace asegúrate hacia dónde va destinado, puedes verlo en la barra de estado del navegador

Cuando colocamos el cursor sobre un enlace en la parte inferior de la ventana (la barra de estado) aparece la dirección hacia la cual dirige el enlace.

El Phishing intenta engañarnos de muchas formas. La forma más común es enviando un mail para una supuesta actualización de datos o contraseña, en donde nos intentaran persuadir a hacer clic en una dirección falsa (incluso con el dominio original de la entidad, como el Banco Francés, HSBC, etc). Al entrar en la falsa pagina uno pone los datos y obviamente no pasara nada o incluso hasta aparezca un mensaje de que la operación se realizo satisfactoriamente. Sin quererlo hemos dado los datos de nuestra cuenta a un ladrón que las usara para robarnos dinero.

Ante cualquier duda sobre estos mails, recomendamos consultarlo a alguno de los teléfonos de dichas entidades para confirmar la veracidad de los mismos.

Puedes utilizar también la barra de Google para detectar estos intentos de fraude, si en algún momento llegas a visitar una página que no se corresponda con la de la entidad real aparecerá este mensaje:

De todas formas, este anuncio no siempre se muestra, por lo que aun así deberás tener mucha cautela a la hora de navegar.