

GUÍA DE CÓMPUTO SEGURO

Al momento en que su sistema esta conectado a la red y/o a Internet, usted esta probablemente beneficiándose de servicios de acceso para mejorar la productividad e incremento de la vida. Enviando y recibiendo correos electrónicos, chateando en línea con amigos, navegando en Internet a través de navegadores de web, y descargando datos o archivos de programas son unas cuantas de las actividades más comunes que además exponen a los sistemas a amenazas de código malicioso como virus y Troyanos.

El poder de las redes de hoy en día pueden fácilmente accesar información útil y hacerlo víctima de virus que se oculten en archivos adjuntos de correo electrónico. Es muy fácil el disparar de manera inadvertida virus sofisticados que serán auto-enviados como correo masivo, e infectando a sus amigos, clientes y colegas de cómputo. En el mundo global real, los brotes de virus como W97M_Melissa, VBS_Loveletter (a.k.a. LoveBug), VBS_Fireburn, W97M_Resume and VBS_Newlove han mostrado que tan efectiva puede ser la tecnología de código malicioso. Hay mas de 50,000 virus hoy en día, nuevos virus pueden surgir diariamente, cualquiera de ellos puede convertirse en el siguiente virus LoveBug!.

Para reducir el riesgo de infección de virus y del disparo inadvertido o esparcimiento de ellos a otra gente, Trend Micro quiere compartir con usted algunas prácticas de “cómputo seguro” que son fácilmente implementadas. Póngalas en práctica en su máquina el día de hoy y estas le ayudarán para tener el acceso a la tecnología de información sin caer presa de virus o algún otro código malicioso.

Para hacer su sistema mas robusto, siga las prácticas marcadas a continuación para ajustar y configurar su sistema. La idea en general es hacer mas difícil o imposible que los virus corran o se ejecuten.

Deshabilite la funcionalidad del host de Windows Scripting (ejecución de scripts)

Esto es para prevenir virus de tipo script de Visual Basic como VBS_LoveLetter corran en su sistema, para que no puedan activarse, esparcirse o causar daño a los archivos. Una PC típica no necesita Windows Scripting Host (WSH) para funcionar normalmente. Usted puede siempre cambiar su opinión y posteriormente reinstalar WSH repitiendo estos pasos y re-seleccionando la opción de “Windows Scripting Host”

Sistema Windows 98

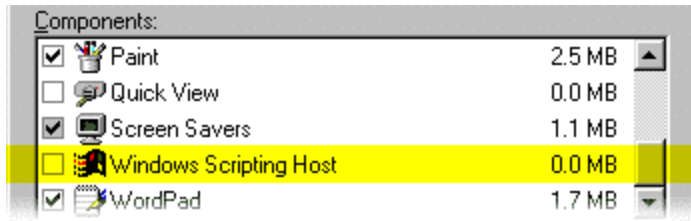
WSH es instalado por default cuando usted instala Windows)(o Internet Explorer 5. Para prevenir que corran los scripts (archivos .VBS)

- Abra el panel de control seleccionando “Inicio”
- Parámetros” y después “Panel de Control”
- De un doble clic en “Agregar/remover Programas”

Seleccione la pestaña de “Configuración de Windows”



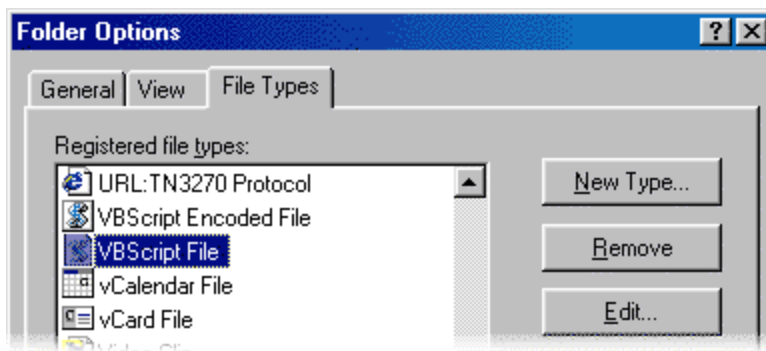
- De un doble clic en “Accesorios”
- Desmarque “WSH”
- Clic en el botón de “OK”



Sistemas Windows 95

Los sistemas de Windows 95 no vienen con WSH. Sin embargo, el WSH es instalado automáticamente cuando instala el Internet Explorer 5 o posterior. Para deshabilitar scripts (con la extensión .VBS) que corran en sistemas Windows 95:

- a. Inicie el Explorador de Windows
(Para hacer esto, seleccione “Inicio”, “Programas” y después “ Explorador de Windows”. Por favor note que este no es lo mismo que el Internet Explorer.)
- b. Seleccione “Ver” y después seleccione “Opción”
- c. Seleccione la pestaña “Tipos de Archivo”
- d. Buscar y seleccionar “Archivo de Script VBScript”
- e. Clic en “Delete” y entonces confirme la remoción seleccionando “Si”

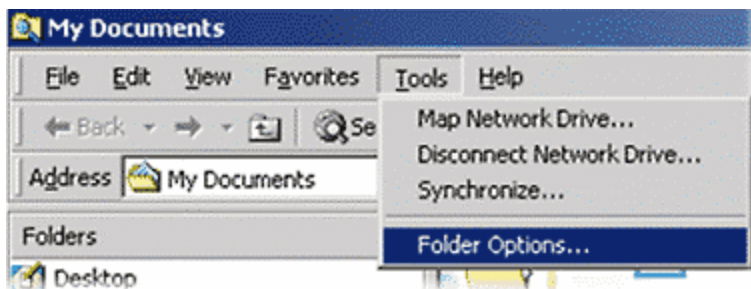


Sistemas Windows 2000

El WSH esta instalado por default en los sistemas Windows 2000.

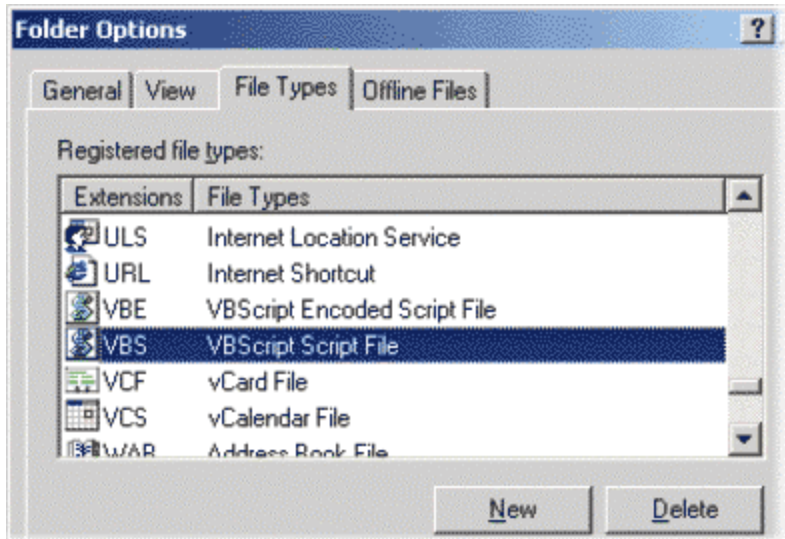
Para deshabilitar los scripts (con extensiones .VBS) de un sistema que este corriendo Windows 2000:

- a. Inicie el Explorador de Windows
- b. Seleccione “Herramientas” y después “Opciones de Directorio”



- c. Seleccione la pestaña de “Tipos de Archivos”

- d. Busque y seleccione “Archivo de Script VBScript”
- e. Dé un clic en “Borrar” y después confirme la remoción seleccionando “Si”

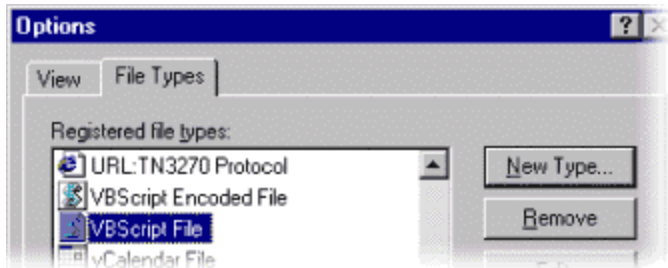


Sistemas Windows NT

Los sistemas de Windows NT no vienen con el WSH. Sin embargo, el WSH es instalado automáticamente cuando usted instala el Internet Explorer 5 o posterior.

Para deshabilitar scripts (con la extensión .vbs) de sistemas que estén corriendo Windows NT 4:

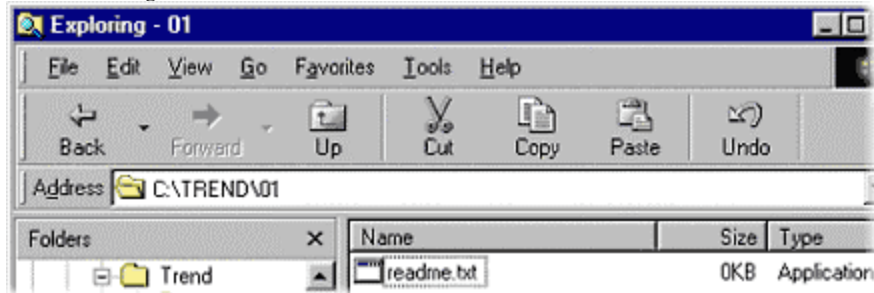
- a. Autentíquese con derechos de Administrador
- b. Inicie el Explorer de Windows
- c. Seleccione “Ver” y después “Opciones”
- d. Seleccione la pestaña de “Tipos de Archivos”
- e. Busque y seleccione “Archivo VBScript”
- f. De un clic en “Remover” y después confirme la remoción seleccionando “Si”



No oculte la extensión de archivos de tipos de archivos conocidos

Todos los sistemas operativos, por default, ocultan las extensiones de archivos conocidos en el Explorador de Windows. Esta característica puede ser usada por los creadores de virus y hackers para ocultar programas maliciosos con algún otro formato, como son texto, video o archivos de audio. Por ejemplo, un archivo de programa malicioso nombrado “readme.txt.exe” es desplegado como “readme.txt” en el Explorador de Windows (verla ilustración abajo).

Sin embargo los usuario son normalmente engañados dentro del tipo de archivo “texto” y después inadvertidamente correr el archivo de código malicioso.



Para evitar esta confusión, se recomienda que cambie los parámetros del Explorador de Windows a “No ocultar la extensión de los tipos de archivos conocidos”. Esto puede ser logrado dando un clic en uno de los siguientes archivos y salvándolo en su disco duro local, después dando un doble-click en el archivo para correr:

Usuarios de Windows 95,98 y de NT 4:



NotHideFileExt_Win9598NT4.reg

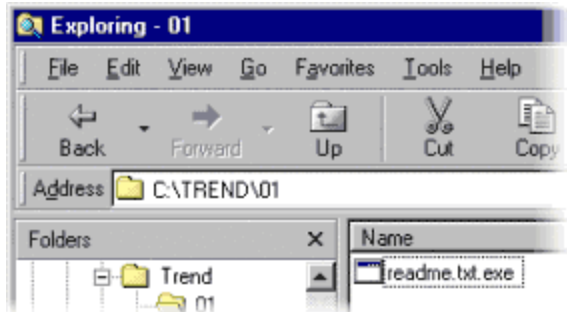
Usuarios de Windows 2000:



NotHideFileExt_Win2000.reg

NOTA: Si usted tiene problemas descargando o si usted recibe un error, descargue las versiones compactadas de estos archivos de registro [aquí](#).

Después, los archivos serán desplegados con le extensión completa del archivo como se muestra:



Nota importante: Existen algunas extensiones de archivos, que el sistema operativo Windows siempre ocultará, como son los archivos de “shell scrap” con las extensiones .shs.

Establezca los parámetros de seguridad del Explorer al menos al nivel Medio

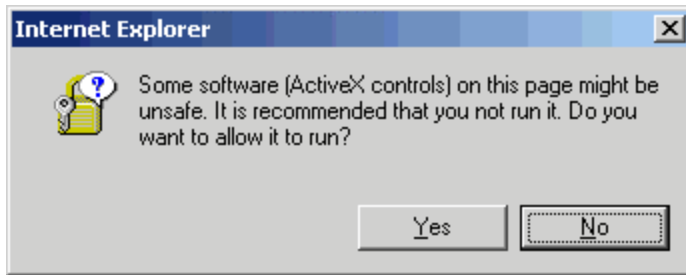
Por default, los parámetros de seguridad del Internet Explorer esta establecida a “Medio”. Sin embargo Trend ha visto muchos sistemas en el que la seguridad ha cambiado a “Bajo”, por un virus, Troyano o hacker.



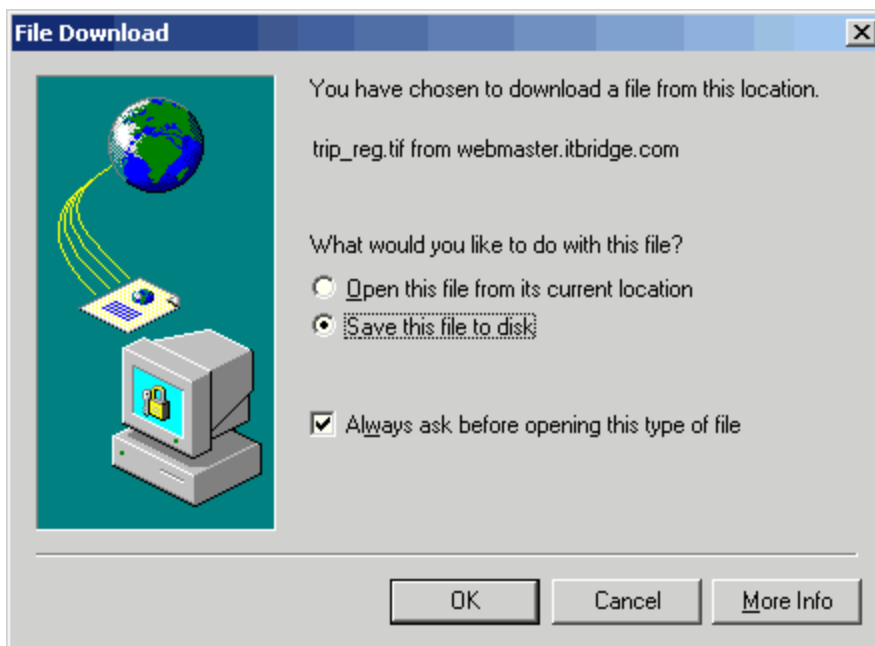
En este respecto, nosotros fomentamos que cada usuario se asegure de que su parámetro de seguridad este configurado al menos en nivel “Medio”, de esta manera se reducirá el riesgo de correr un archivo malicioso accidentalmente.

En el nivel de seguridad “Medio”, Internet Explorer 5 preguntará a los usuarios antes de correr un contenido potencialmente no seguro.

Internet Explorer 5 o posterior desplegará un mensaje de advertencia antes de correr cualquier control de Active-X (como se muestra en la figura siguiente)



Nosotros también advertimos que los usuarios siempre salven los archivos a la unidad del disco local y después los escanee con un producto antivirus actualizado. Si usted no tiene un producto antivirus o si su producto está caducado, por favor utilice el escáner gratuito de Trend Micro "HouseCall" desde <http://housecall.antivirus.com>



Para automáticamente cambiar el parámetro del Internet Explorer 5 al nivel "Medio", por favor ejecute el siguiente archivo de registry:



NOTA: Si usted tiene problemas descargando o si usted recibe un error, descargue las versiones compactadas de estos archivos de registry [aquí](#).

Configure que pida una confirmación antes de abrir un archivo anexo de un correo (aplica a usuarios de Microsoft Outlook y Outlook Express)

Nosotros hemos visto muchos virus activados porque los usuarios hicieron un doble clic en un archivo anexo en un correo electrónico recibido. En este caso, nosotros advertimos que los usuarios de internet guarden sus archivos a la unidad de disco duro local y después los escanee con un producto antivirus actualizado (en lugar de da un doble clic sobre el archivo adjunto al correo electrónico)

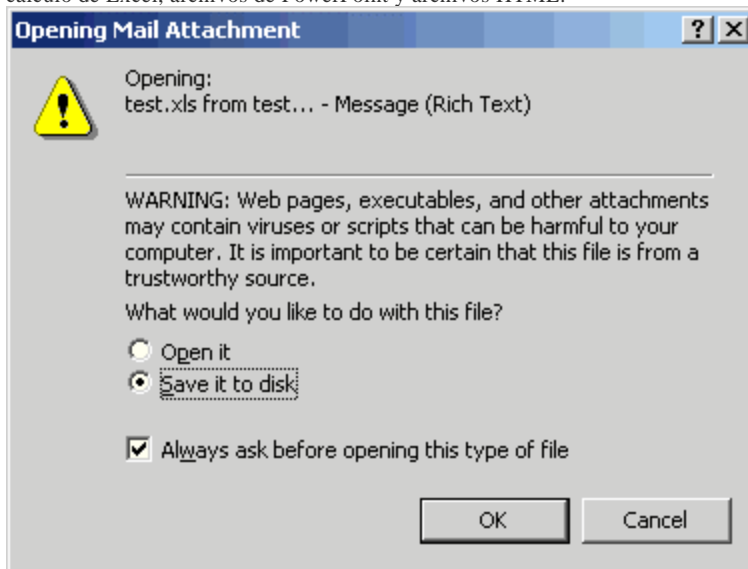
Para asegurar que su sistema automáticamente pregunte para salvar los archivos, por favor de un clic en el archivo que se encuentra a continuación, y sávelo en su disco duro local, después de un doble clic en el archivo para ejecutarlo:



WarnMailAttachment.reg

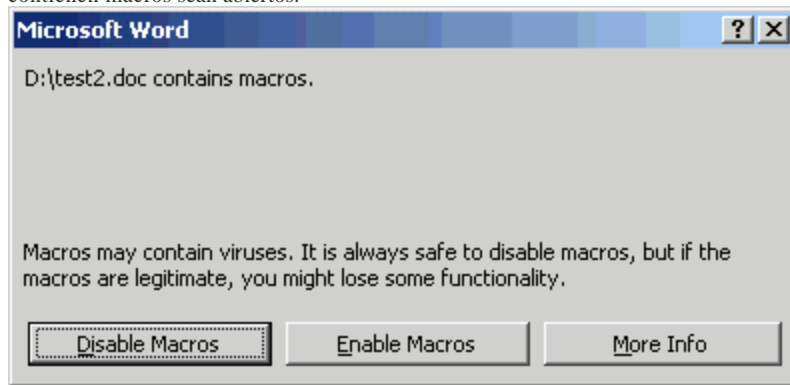
NOTA: Si usted tiene problemas descargando o si usted recibe un error, descargue las versiones compactadas de estos archivos de registry aquí.

Después de esto, su sistema preguntará con un aviso si usted accidentalmente da un clic en un archivo anexo del correo electrónico o lee algún archivo que tiene integrados scripts. Este arreglo al registry aplica a documentos Word, hojas de cálculo de Excel, archivos de PowerPoint y archivos HTML.



Active alertas de virus tipo Macro en MS Office97 y 2000
(aplica a usuarios de Office 97 y 2000)

Por default, los productos de Microsoft Office despliegan una advertencia de Macro antes de que los documentos que contienen macros sean abiertos.



Sin embargo, muchos de los virus tipo macro deshabilitan este parámetro para evitar ser detectados. Para asegurar que usted tiene la advertencia de macro activa, por favor de un clic en uno de los siguientes archivos que se muestran a continuación, y guárdelo en su disco duro local, posteriormente de un doble clic en el archivo para ejecutarlo:

Usuarios de Microsoft office 97 (a.k.a. Office 8.0):



MacroWarning_Office8.reg

Usuarios de Microsoft Office 2000 (a.k.a. Office 9.0):



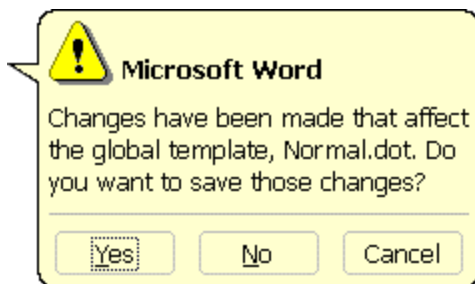
MacroWarning_Office9.reg

NOTA: Si usted tiene problemas descargando o si usted recibe un error, descargue las versiones compactadas de estos archivos de registry aquí.

Si usted no esta seguro si el contenido de una macro que haya encontrado es segura, nosotros recomendamos usar las opción "Deshabilitar macros"

Pida confirmación antes de salvar los cambios a una plantilla global
(normal.dot – aplica a Usuarios de Word 97 y Word 2000)

Debido a que todos los virus de tipo macro intentan modificar la plantilla global (normal.dot) antes de cerrar la sesión activa de Microsoft Word, nosotros recomendamos a todos que se aseguren que Microsoft Word preguntará antes de que cualquier cambio sea hecho.



Mientras que esta acción no para a todos los virus tipo macro, esto le ayudará a identificar código potencialmente malicioso.

Si usted no esta seguro de que hacer, seleccione la opción "No" y envíe una copia vía correo electrónico a los doctores de virus de Trend Micro a virus_doctor@trendmicro.com . Ellos inspeccionarán los archivos sospechosos o documentos para determinar si estos contienen macros maliciosos. Para hacer el cambio a Word 97 o Word 2000 automáticamente, por favor de un clic en uno de los siguientes archivos que se encuentran a continuación, y guárdelo en su disco duro local, después de un doble clic en el archivo para que se ejecute:

Usuarios de Word 97 (a.k.a. Word 8.0):



TmplateSavePrompt_W8.reg

Usuarios de Word 2000 (a.k.a. Word 9.0):



TmplateSavePrompt_W9.reg

NOTA: Si usted tiene problemas descargando o si usted recibe un error, descargue las versiones compactadas de estos archivos de registry aquí.

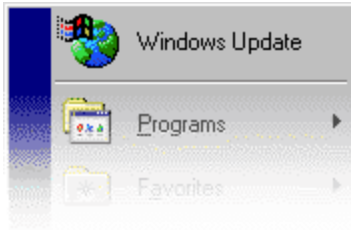
Aplique las últimas actualizaciones de seguridad de Microsoft

Para cerrar los huecos de seguridad que se han descubierto desde que Windows fue enviado e instalado, nosotros recomendamos a todos visitar el sitio web de actualización de Microsoft en <http://windowsupdate.microsoft.com>

Por favor siga las instrucciones en línea en como actualizar su sistema. Las actualizaciones de seguridad le ayudarán en prevenir que los hacker accedan a su sistema y previene que los virus corran en su sistema.

Los usuarios de Windows 98 o Windows 2000 pueden adicionalmente usa la característica de Windows Update (Actualizaciones de Windows) para obtener todas las últimas actualizaciones de seguridad.

Simplemente de un clic en "Inicio" y después seleccione "Actualizaciones de Windows"



Conclusiones:

Las practicas de cómputo seguro principalmente hacen mas difícil la entrada o ejecución de código malicioso en el sistema del cliente. Sin embargo, las prácticas recomendadas de cómputo seguro no tienen el objeto de remplazar un software antivirus actualizado.

Los usuarios de sistemas que han sido atacados por virus o Troyanos pueden decirle historias respecto a los problemas que se pueden enfrentar como mínimo – o respecto a los datos importantes que ellos han perdido. En general, la mayoría de los virus son puras molestias, pero cada vez surge un nuevo virus que puede venir con una nueva técnica y causar un daño mayor a las computadoras o amenazar los datos o la seguridad de los datos.

Estas prácticas de cómputo seguro crearán una capa protectora de defensa para prevenir que los virus corran de manera inadvertida.

Otros recursos:

- Para todos los usuarios de Internet, Trend Micro ofrece un escaner actualizado en línea llamado [HouseCall](#).
- Los usuarios que sospechen que un archivo tenga un virus o troyano pueden enviar una muestra a la dirección de correo electrónico virus_doctor@trendmicro.com para que un grupo de doctores en virus lo revise. Este es un servicio gratuito provisto por Trend Micro.
- Último [antivirus e información de seguridad en contenido](#)
- Último patrón de archivos para los [productos antivirus de Trend Micro](#)