

SEGURIDAD INFORMATICA CONTRA VIRUSES Y OTRAS AMENAZAS

INDICE

1. ¿Que son los virus informáticos? ➡
2. ¿Qué es un gusano? ➡
3. ¿Qué es un troyano? ➡
4. ¿Qué clases de virus existen? ➡
5. ¿Qué tipo de virus de acuerdo a la selección anterior, es el más peligroso? ➡
6. ¿Cuáles son los medios de entrada de los virus a mi computador? ➡
7. ¿Qué es el Spam? ➡
8. ¿Qué es el phishing? ➡
9. ¿Cómo puedo proteger mi computador? ➡
10. ¿Cómo prevenir virus que provengan del correo electrónico? (Datos Adjuntos) ➡
11. ¿Qué consideraciones mas debo tener en cuenta para que mi maquina no sea infectada? ➡
12. ¿Qué es un antivirus? ➡
13. ¿Existe algún antivirus 100% eficiente? ➡
14. ¿Cuáles son los Antivirus más conocidos o populares? ➡
15. ¿Cómo son los Pasos Básicos para limpiar el computador cuando está infectado? ➡
16. ¿Cuáles son los Antivirus y herramientas gratuitas para limpiar el computador? ➡
17. ¿Que son los Backups o copias de respaldo, para qué sirven? ➡

1. ¿Que son los virus informáticos?

Los virus informáticos son programas que se copian de forma automática y que su objetivo es afectar el normal funcionamiento de una computadora, sin el consentimiento del usuario.

En el sentido estricto del término, los virus informáticos son programas que pueden replicarse y ejecutarse por sí mismos. En su accionar, suelen reemplazar archivos ejecutables del sistema por otros infectados con el código maligno. Los virus pueden simplemente molestar al usuario, bloquear las redes al generar tráfico inútil o, directamente, destruir los datos almacenados en el disco duro del computador.

El virus se adjunta a sí mismo a un programa o archivo para propagarse de un equipo a otro. Infecta a medida que se transmite. Los virus pueden dañar el software, el hardware y los archivos.

Los virus se introducen en nuestras computadoras de forma muy diversas, con la finalidad de producir efectos no deseados y nocivos.

Cada vez que un virus entra en nuestra PC diremos que se ha producido una infección. El 'virus ideal' (desde el punto de vista de los autores de virus) sería aquel que se propaga de forma sigilosa, sin que nadie lo advierta, e inicia su actividad destructiva una vez que las computadoras se encuentran ya infectadas.

Uno de ellos, a modo de ejemplo entre los miles que existen, es el SirCam, que en cuestión de horas infectó cientos de miles de PCs en Latinoamérica. Entre otros ejemplos de virus tenemos: Y2K, CIH, Redlof, Win32, Valentin.E, etc.



2. ¿Qué es un gusano?

Un gusano, al igual que un virus, está diseñado para copiarse de un equipo a otro, pero lo hace automáticamente. En primer lugar, toma el control de las características del equipo que permiten transferir archivos o información. Una vez que un gusano esté en su sistema, puede viajar solo. El gran peligro de los gusanos es su habilidad para replicarse en grandes números. Por ejemplo, un gusano podría enviar copias de sí mismo a todos los usuarios de su libreta de direcciones de correo electrónico, lo que provoca un efecto dominó de intenso tráfico de red que puede hacer más lentas las redes empresariales e Internet en su totalidad. Cuando se lanzan nuevos gusanos, se propagan muy rápidamente. Bloquean las redes y posiblemente provocan esperas largas (a todos los usuarios) para ver las páginas Web en Internet.

El gusano es una subclase de virus. Por lo general, los gusanos se propagan sin la intervención del usuario y distribuye copias completas (posiblemente modificadas) de sí mismo por las redes. Un gusano puede consumir memoria o ancho de banda de red, lo que puede provocar que un equipo se bloquee.



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574

Debido a que los gusanos no tienen que viajar mediante un programa o archivo "host", también pueden crear un túnel en el sistema y permitir que otro usuario tome el control del equipo de forma remota. Entre los ejemplos de gusanos se incluyen: *Sasser*, *Blaster*, *Iloveyou*, *Melissa*, etc.



3. ¿Qué es un troyano?

Del mismo modo que el caballo de Troya mitológico parecía ser un regalo pero contenía soldados griegos que dominaron la ciudad de Troya, los troyanos de hoy en día son programas informáticos que parecen ser software útil pero que ponen en peligro la seguridad y provocan muchos daños. Un troyano reciente apareció como un mensaje de correo electrónico que incluye archivos adjuntos que aparentaban ser actualizaciones de seguridad de Microsoft, pero que resultaron ser virus que intentaban deshabilitar el software antivirus y de servidor de seguridad.

Un troyano es un programa informático que parece ser útil pero que realmente provoca daños.

Los troyanos también se pueden incluir en software que se descarga gratuitamente. Nunca descargue software de un origen en el que no confíe. Descargue siempre las actualizaciones y revisiones de Microsoft de los sitios Microsoft Windows Update o Microsoft Office Update, en caso que su sistema operativo sea Microsoft Windows. Entre los ejemplos de troyanos tenemos: *agent*, *excecutor*, *eva xp 1*, *happy99*, etc.



4. ¿Qué clases de virus existen?

La clasificación de los virus se puede realizar en función del medio empleado y las técnicas utilizadas por éstos para extenderse.

Así, existen varios tipos:

Viruses Residentes. Se colocan automáticamente en la memoria de la computadora y desde ella esperan la ejecución de algún programa o la utilización de algún archivo.

Viruses de Acción Directa. Los virus que se pueden englobar en este grupo, realizan copias de sí mismos a las computadoras que infectan.

Viruses de Sobreescritura. Sobrescriben en el interior de los archivos atacados, haciendo que se pierda el contenido de los mismos.

Viruses de Boot. Atacan a los disquetes y discos duros, haciendo imposible su utilización.



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574

Viruses de Macro. Estos virus infectan los archivos de texto, Bases de Datos, presentaciones, etc., que incluyen en ellos pequeños programas llamados macros, que permiten realizar algunas acciones de forma automática.

Viruses de Enlace o Directorio. Modifican las direcciones que permiten, a nivel interno, acceder a cada uno de los archivos existentes. El resultado es que posteriormente será imposible localizarlos y trabajar con ellos.



5. ¿Qué tipo de virus de acuerdo a la selección anterior, es el más peligroso?

De acuerdo con la International Security Association, los virus macro forman el 80% de todos los virus y son los que más rápidamente han crecido en toda la historia de los ordenadores en los últimos 5 años. A diferencia de otros tipos de virus, los virus macro no son exclusivos de ningún sistema operativo y se diseminan fácilmente a través de archivos adjuntos de e-mail, disquetes, bajadas de Internet, transferencia de archivos y aplicaciones compartidas.

Los virus macro son, sin embargo, aplicaciones específicas. Infectan las utilidades macro que acompañan ciertas aplicaciones como el Microsoft Word y Excel, lo que significa que un word virus macro puede infectar un documento Excel y viceversa.

En cambio, los virus macro viajan entre archivos en las aplicaciones y pueden, eventualmente, infectar miles de archivos.

Los virus macro son escritos en Visual Basic y son muy fáciles de crear. Pueden infectar diferentes puntos de un archivo en uso, por ejemplo, cuando éste se abre, se graba, se cierra o se borra. Lo primero que hacen es modificar la plantilla maestra (normal.dot) para ejecutar varias macros insertadas por el virus, así cada documento que abramos o creamos, se incluirán las macros "víricas".



6. ¿Cuáles son los medios de entrada de los virus a mi computador?

Para realizar sus infecciones y lograr sus objetivos, emplean diferentes medios de entrada en nuestras computadoras.

Estos pueden ser los siguientes:

- ✓ **Unidades de Disco:** Floppy Disk, Lectores de CD o DVD.
- ✓ **Puertos USB:** Flash Memory o PenDrive, Discos Duros Flexibles
- ✓ **Redes de Computadoras.**
- ✓ **Internet:** Correo electrónico, IRC o Chat, Páginas Web., Transferencia de Archivos (FTP) y/o Grupos de Noticias y descarga de archivos.



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574

7. ¿Qué es el Spam?

Simplemente se denomina con este término al correo electrónico (E-mail) que se recibe de forma indeseada, estos mensajes, habitualmente de tipo comercial, no son solicitados y son enviados en cantidades masivas a muchos usuarios a la vez.

Los siguientes son ejemplos típicos de correo spam:

- Trabajar desde la casa
- Perder peso o curas milagrosas
- Contenido para adultos
- Casinos virtuales

Mensajes en cadena

Este tipo de Spam, llega en forma de mensajes en cadena que incluyen temas como por ejemplo: ayuda a víctimas de enfermedades o accidentes, dinero fácil, medicinas milagrosas, religión, política y pornografía.

Es muy común encontrarse con estos correos en forma de cadena que lo único que buscan es su dirección de correo electrónico para enviar más Spam y saturar la red.

Existen cadenas muy interesantes las cuales podemos compartir con nuestros conocidos, amigos o familiares, una forma muy fácil de evitar el Spam es escribir la lista de destinatarios en la casilla de CCO (con copia oculta) en el correo electrónico.



8. ¿Qué es el phishing?

El "phishing" es una modalidad de estafa diseñada con la finalidad de robarle la identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como su banco o la empresa de su tarjeta de crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aun más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574

al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Procedimientos para protegerse del "phishing"

Sale la pregunta al aire, ¿de qué forma me protejo del phishing? Al igual que en el mundo físico, los estafadores continúan desarrollando nuevas y más siniestras formas de engañar a través de Internet. Si sigue estos cuatro sencillos pasos podrá protegerse y preservar la privacidad de su información.

1. Nunca responda a solicitudes de información personal a través de correo electrónico. Si tiene alguna duda, póngase en contacto con la entidad que supuestamente le ha enviado el mensaje.
2. Para visitar sitios Web, introduzca la dirección URL en la barra de direcciones.
3. Asegúrese de que el sitio Web utiliza cifrado.
5. Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.

Paso 1: nunca responda a solicitudes de información personal a través de correo electrónico

Microsoft y las empresas de prestigio nunca solicitan contraseñas, números de tarjeta de crédito u otro tipo de información personal por correo electrónico. Si recibe un mensaje que le solicita este tipo de información, no responda. Si piensa que el mensaje es legítimo, comuníquese con la empresa por teléfono o a través de su sitio Web para confirmar la información recibida.

Paso 2: para visitar sitios Web, introduzca la dirección URL en la barra de direcciones

Si sospecha de la legitimidad de un mensaje de correo electrónico de la empresa de su tarjeta de crédito, banco o servicio de pagos electrónicos, no siga los enlaces que lo llevarán al sitio Web desde el que se envió el mensaje. Estos enlaces pueden conducirlo a un sitio falso que enviará toda la información ingresada al estafador que lo ha creado.

Paso 3: asegúrese de que el sitio Web utiliza cifrado

Si no se puede confiar en un sitio Web por su barra de direcciones, ¿cómo se sabe que será seguro? Existen varias formas: En primer lugar, antes de ingresar cualquier tipo de información personal, compruebe si el sitio Web utiliza cifrado para transmitir la información personal. En Internet Explorer puede comprobarlo con el icono de color amarillo situado en la barra de estado, tal como se muestra en la figura.



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574



Icono de candado de sitio seguro. Si el candado está cerrado, el sitio utiliza cifrado.

Este símbolo significa que el sitio Web utiliza cifrado para proteger la información personal que introduzca: números de tarjetas de crédito, número de la seguridad social o detalles de pagos.

Haga doble clic sobre el icono del candado para ver el certificado de seguridad del sitio. El nombre que aparece a continuación de **Enviado a** debe coincidir con el del sitio en el que se encuentra. Si el nombre es diferente, puede que se encuentre en un sitio falso. Si no está seguro de la legitimidad de un certificado, no introduzca ninguna información personal. Sea prudente y abandone el sitio Web.

Paso 5: comuníquese los posibles delitos relacionados con su información personal a las autoridades competentes

Si cree que ha sido víctima de "phishing", Informe inmediatamente del fraude a la empresa afectada y las autoridades competentes.

A continuación podemos ver un ejemplo de phishing, a simple vista parece ser la página de inicio de Hotmail, pero si observamos con atención algunos detalles como la URL, veremos que esta no tiene relación alguna con Hotmail o Windows Live:



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574

Otro ejemplo clásico es el siguiente:



9. ¿Cómo puedo proteger mi computador?

Nada puede garantizar la seguridad del equipo de forma absoluta. No obstante, puede reforzar la seguridad de su equipo con los siguientes 4 pasos básicos.

1. Use Cortafuegos o firewall
2. Mantenga al día su sistema operativo
3. Instale y actualice su antivirus



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574

4. Instale y actualice su programa antispyware

1. Cortafuegos o firewall

Software o hardware que puede ayudar a proteger un equipo contra piratas informáticos o software malintencionado. El cortafuegos o firewall crea una barrera entre su computador e Internet. Es como un chequeo de seguridad por el cual tienen que pasar todos los programas y la información antes de que les sea permitido entrar a su computador.

El cortafuegos es la primera línea de defensa que protege su computador, ya que ayuda a hacerlo invisible a los criminales en línea y a muchos tipos de software dañino, como los virus y los gusanos. El cortafuegos también puede ayudar a prevenir que los programas instalados en su computador acepten actualizaciones desde Internet sin su permiso.

2. Mantenga al día su sistema operativo

Una de las cosas más importantes que puede hacer para proteger su computador es también una de las más simples: mantener su sistema operativo al día con las últimas actualizaciones de software disponibles.

Los criminales en línea están constantemente trabajando en nuevas formas de atacar su computador y de invadir su privacidad. Afortunadamente, las compañías de software trabajan aún más duro para contrarrestar esas amenazas y proporcionarle las herramientas más modernas para proteger su computador.

Usted debe actualizar el sistema operativo de su computador regularmente con las actualizaciones de seguridad que le proporciona el fabricante. Lo mismo aplica para los navegadores de internet y otros programas, incluyendo el antivirus y el anti-spyware. La mayoría de estas actualizaciones están disponibles a través de suscripciones ofrecidas por los fabricantes.

3. Instale y actualice un antivirus

Los programas antivirus ayudan a proteger su computador escaneando cada correo electrónico, programa o contenido que entra en su computador. Los programas antivirus más potentes pueden detectar y destruir cientos de virus específicos antes de que tengan la oportunidad de dañar su sistema.

Los criminales de internet están constantemente creando nuevos virus y gusanos, inventando nuevas formas de invadir y dañar su computador. Para proteger su computador de estas amenazas, asegúrese de que nunca deje que su antivirus expire, y mantenga su software al día con las últimas actualizaciones del fabricante.

4. Instale y actualice un programa antispyware

Los programas antispyware pueden mostrarle algunos programas espías que ya están en su sistema y ayudarlo a mantener su computador alerta para prevenir otras intromisiones futuras. Al igual que con su sistema operativo y su antivirus, es esencial mantener los



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574

programas antispyware actualizados para asegurar que cuenta con los mejores niveles de protección.



10. ¿Cómo prevenir virus que provengan del correo electrónico? (Datos Adjuntos)

Siga estos pasos básicos cuando reciba un archivo adjunto a un mensaje, sin importar el programa de correo electrónico que utilice:

1. No abra ningún archivo adjunto si no conoce al remitente y no lo esperaba.
2. Si recibe un mensaje de correo electrónico con un archivo adjunto de algún remitente desconocido, elimínelo de inmediato.
3. Utilice software antivirus y manténgalo actualizado.
4. Si debe enviar un archivo adjunto, prevenga al destinatario para que no lo confunda con un virus.
5. Utilice filtros contra correo no deseado para bloquear los mensajes de correo no deseados, muchos de los cuales contienen archivos adjuntos peligrosos.



11. ¿Qué consideraciones mas debo tener en cuenta para que mi maquina no sea infectada?

Los virus por lo habitual traen extensiones diferentes a la que estamos acostumbrados o que usualmente utilizamos, como ejemplo de extensiones conocidas o bajo riesgo podrían ser: *.jpg, *.gif, *.bmp, *.pdf, *.psd, *.mp3, *.mpeg, *.avi, *.mov, *.doc, etc.

Las extensiones de los virus suelen ser las siguientes: *.exe, *.com, *.pif, *.bat, etc.

Entonces cabe tener cuidado a revisar la extensión de todo lo recibido vía Email, otros cuidados a tener son los virus que vienen camuflados para confundir a las personas y que piensen que es simplemente una foto o un tema musical o un link, por ejemplo: **mifoto.jpg.exe**, **micancionfavorita.mp3.pif** la extensión que es verdadera es la del final.

A su vez hay que tener cuidado con los links que nos envían por correo electrónico o chat. Por ejemplo tenemos:

“El joven que aparece en la fotografía se parece mucho a ti, me parece gracioso, por favor abre la foto haciendo clic en el link de abajo”

Link: <http://192.168.15.54/fotogrupal.exe>

O directamente cuando navegamos por diferentes páginas en internet nos encontramos toda clase de mensajes, banners, fotografías para clikear, estos a su vez pueden estar



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574

alojando virus potenciales riesgosos y la infección se produce simplemente al hacer clic sobre ellos, los siguientes ejemplos nos dan una pauta de una posible infección de virus:



12. ¿Qué es un antivirus?

Un antivirus es un programa creado para prevenir o evitar la activación de los virus, así como su propagación y contagio. Cuenta además con rutinas de detención, eliminación y reconstrucción de los archivos y las áreas infectadas del sistema.

Un antivirus tiene tres principales funciones y componentes:

- **Vacuna**, es un programa que instalado residente en la memoria, actúa como "filtro" de los programas que son ejecutados, abiertos para ser leídos o copiados, en tiempo real.
- **Detector**, que es el programa que examina todos los archivos existentes en el disco o a los que se les indique en una determinada ruta o PATH. Tiene instrucciones de control y reconocimiento exacto de los códigos virales que permiten capturar sus



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574

pares, debidamente registrados y en forma sumamente rápida desarman su estructura.

- **Eliminador**, es el programa que una vez desactivada la estructura del virus procede a eliminarlo e inmediatamente después a reparar o reconstruir los archivos y áreas afectadas.



13. ¿Existe algún antivirus 100% eficiente?

La respuesta es NO, no existe un antivirus 100% eficaz, hay que tener en cuenta que uno bueno debe ser capaz de detectar cualquier código extraño o malicioso que intente ingresar a un sistema informático. Debe proteger cuando estemos navegando en la red, cuando introducimos algún medio portátil o CD/DVD, o cuando nuestro computador este en red con otros computadores, básicamente.



14. ¿Cuáles son los Antivirus más conocidos o populares?

Existen muchas compañías que se desarrollan antivirus y productos de seguridad, entre los antivirus más populares están:

- Norton Antivirus
- Mcaffé
- Panda
- AVG
- NOD 32
- Kaspersky
- Avast.



15. ¿Cómo son los Pasos Básicos para limpiar el computador cuando está infectado?

Estos pasos se deben realizar cuando nuestro computador esta diferente en su funcionamiento habitual o normal, entonces deberemos suponer que nuestro computador sufre de alguna infección de virus u otra amenaza, para dar una solución a este problema debemos de seguir las instrucciones siguientes:

1.- Scanea tu computador con un antispyware y antivirus actualizado, si no tienes uno puedes descargar gratuitamente de los siguientes links.

<http://free.avg.com/>

<http://www.malwarebytes.org/>



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574

2.- Si el antivirus no puede remover los virus de tu computador, reinicia en modo seguro (safe mode) e intenta nuevamente scanear todo tu computador. Para ingresar en modo seguro presiona la tecla F8 antes de iniciar Windows.

Existen muchas otras herramientas gratuitas como SmitREM, HijackThis que podrían ayudar a limpiar tu computador.

3.- Si su computador sigue infectado, es recomendable contactar con un técnico especialista, sobre todo si tiene información importante y sensible en su computador.



16. ¿Cuáles son los Antivirus y herramientas gratuitas para limpiar el computador?

Estos son enlaces a sitios web con utilidades gratuitas online, como escaneos de virus, de spyware, de seguridad, etc.

Algunos sitios requieren Internet Explorer, registrarse e instalar complementos ActiveX.

Antivirus online

- * http://old.antivir.ru/english/www_av/
- * <http://www3.ca.com/securityadvisor/virusinfo/scan.aspx>
- * <http://www.freedom.net/viruscenter/...viruscheck.html>
- * <http://www.kaspersky.com/remoteviruschk.html>
- * <http://www.pandasoftware.es/activescan/>
- * <http://pcpitstop.com/antivirus/default.asp>

Nota: algunos de los Links pueden estar caído o sin respuesta, esto es porque algunas páginas cambian sus webs y sus links anteriores dejan de servir.



17. ¿Que son los Backups o copias de respaldo, para qué sirven?

(Copia de seguridad) Es la copia total o parcial de información importante del disco duro, CDs o DVDs, bases de datos u otro medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún otro sistema de almacenamiento masivo, como ser discos duros portátiles, CDs, DVDs, flash drive o sitios en internet diseñados para este fin.

Los backups se utilizan para tener una o más copias de información considerada importante y así poder recuperarla en el caso de pérdida de la copia original.



www.AsistenciaRemota24.com

Móvil: 07904222132

Teléf.: 02071934574