Seguridad informática educativa

Cómo protegerse de los virus informáticos

2002-12-01

Cómo protegerse de los virus informáticos

> *Normas básicas para evitar contaminarse con los virus informáticos. Se acompañan de la reseña de algunos programas Antivirus descargables de la Red.*

Normas básicas para evitar contaminarse con los virus informáticos. Se acompañan de la reseña de algunos programas Antivirus descargables de la Red.

CÓMO PROTEGERSE DE LOS VIRUS INFORMÁTICOS

Los Virus informáticos se han convertido en una continua pesadilla, especialmente, para los usuarios del correo electrónico. Es muy probable que usted o algún conocido suyo haya sido victima de estos molestos ‘bichos’ informáticos que aparecen donde uno menos lo espera.

Para propagar sus creaciones y lograr sus fines, quienes se dedican a fabricar Virus frecuentemente apelan a inclinaciones emocionales profundas de sus posibles victimas como: el miedo, la curiosidad, el deseo, el sexo, la codicia, la compasión o incluso la bondad natural, para lograr sus fines.

Muchas veces advierten a su victima mediante un correo electrónico en el que le comunican que tiene infectado el computador con un peligroso virus que borrará toda la información contenida en el disco duro. Muy amablemente ofrecen el software que solucionará el problema o una dirección de Internet desde la cual éste se puede

descargar. Lo cierto es que cuando la victima ejecuta esos programas, se activa el verdadero virus o queda desprotegido el computador para que ingresen los ‘crackers’ [1] quienes lo puedan utilizar, sin ser descubiertos, para atacar sistemas de terceros.

En otros casos se aprovechan de la curiosidad e ignorancia de su victima para lograr que ésta abra un mensaje de correo electrónico infectado, con argumentos como que al abrirlo podrá ver fotos de alguna actriz famosa desnuda o las últimas imágenes de alguna noticia de actualidad. Muchos de estos mensajes provienen de personas conocidas, que ya tienen infectado su computador; de esta forma se evita la desconfianza sobre la autenticidad del mensaje.

Por ejemplo, un gusano [2] llamado “Prestige” se propaga mediante un correo electrónico en cuyo asunto (subject) dice: "fotos INEDITAS del PRESTIGE en el fondo del Atlántico". Sin embargo, lo que realmente incluye el archivo adjunto no son fotos, sino un virus informático. El Virus “SirCam” es otro ejemplo que ha engañado miles de usuarios en todo el mundo. Viene en un archivo adjunto (attachement) a un mensaje de correo electrónico cuyo asunto (subject) dice: "Hola, ¿cómo estás?"; además, se puede leer en el cuerpo del mensaje: "Te mando este archivo para que me des tu punto de vista. Nos vemos pronto". Cuando el usuario abre el archivo para revisarlo y poder así dar una opinión, el virus infecta el computador y se reenvía automáticamente a quienes aparecen en la libreta de direcciones del usuario infectado. Por este motivo, el virus llega remitido regularmente por una persona conocida.

Para su información, seguidamente listamos una serie de normas básicas que le ayudarán a protegerse de los virus informáticos:

- Instale en su computador un software Antivirus confiable (ver lista de opciones en la siguiente sección).

- Actualice con frecuencia su software Antivirus (mínimo dos veces al mes).

- Analice con un software Antivirus actualizado, cualquier correo electrónico antes de abrirlo, así conozca usted al remitente.

- Analice siempre con un software Antivirus los archivos en disquete o Cd-Rom antes de abrirlos o copiarlos a su computador.

- No descargue, ni mucho menos ejecute, archivos adjuntos (attachement) a un mensaje de correo electrónico sin antes verificar con la persona que supuestamente envió el mensaje, si efectivamente lo hizo.

- No ejecute nunca un programa de procedencia desconocida, aun cuando el software Antivirus indique que no está infectado. Dicho programa puede contener un troyano [3] o un sniffer [4] que reenvíe a otra persona su clave de acceso u otra información.

- Instale los parches [5] de actualización de software que publican las compañías fabricantes para solucionar vulnerabilidades de sus programas. De esta manera se puede hacer frente a los efectos que puede provocar la ejecución de archivos con códigos maliciosos.

- Tenga cuidado con los mensajes alusivos a situaciones eróticas (versión erótica del cuento de Blancanieves y los Siete Enanitos, fotos de mujeres desnudas, fotos de artistas o deportistas famosos, etc.).

- Nunca abra archivos adjuntos a un mensaje de correo electrónico cuya extensión [6] sea “.exe”, “.vbs”, “.pif”, “.bat” o “.bak”.

- Cerciórese que el archivo adjunto no tenga doble extensión. Por ejemplo: “NombreArchivo.php.exe”.

- Evite el intercambio por correo electrónico de archivos con chistes, imágenes o fotografías.

- Visite con cierta frecuencia sitios que ofrecen información sobre los últimos virus aparecidos: (http://esp.sophos.com/,http://www.pandasoftware.es/, http://www.deltaasesores.com/recu/RECVirus.html, etc).

- Haga una copia de seguridad de los datos de su computador con la frecuencia que estime más conveniente. De esta forma, si se produce un ataque vírico, es fácil recuperar copias seguras de todos los archivos.

- Suscríbase a un servicio de notificación por correo electrónico de nuevos virus. Enterarse a tiempo de su existencia y de la forma como se comportan es una de los modos más efectivos de evitar un contagio (http://esp.sophos.com/virusinfo/notifications/, http://www.trendmicro.com).

- Si su computador tiene comportamientos extraños y usted sospecha que ha sido infectado por un Virus, visite los sitios Web de los fabricantes de software Antivirus y busque información sobre los nuevos Virus; generalmente, allí se indica como desinfectar el computador.

- La mayoría de las aplicaciones que aceptan código de macro [7] tienen valores de seguridad que se pueden configurar. Si usted usa Internet Explorer, escoja [Herramientas/Opciones de Internet], pulse la pestaña de “Seguridad” y entonces seleccione la “zona de Internet”. Pulse el botón de “Nivel de Seguridad” para examinar las opciones de seguridad, o pulse el botón de “Nivel Prefijado” para asegurar que el nivel de seguridad esté puesto en Mediano. Para encontrar los valores de seguridad de Netscape Navigator, escoja [Editar/Preferencias], y seleccione “Avanzado” en la ventana de Categoría. No olvide los valores de seguridad de macro de su aplicación. En Word, Excel o Outlook 2000, escoja [Herramientas/Macro/Seguridad] y asegúrese de que su

valor esté en “Mediano” o “Alto”.

- No comparta los disquetes. Incluso un amigo bien intencionado puede, sin saberlo, contagiarlo con un virus, un caballo troyano o un gusano. Etiquete sus discos flexibles claramente para que distinga los suyos y no los preste. Si un amigo le presta un disquete que no es suyo, sugiérale un método alternativo para compartir archivos.

- Cuando no entienda algún término utilizado por los expertos en Virus, acuda a los sitios de fabricantes de software Antivirus donde podrá encontrar glosarios de las palabras utilizadas en este sector de la industria informática.

- Desconfíe de mensajes de correo electrónico no solicitados que le ofrecen la oportunidad de descargar software para intercambiar música, programas antivirus o fotografías.

- No haga caso a los mensajes tipo cadena que ofrecen instrucciones para borrar un archivo de su computador argumentando que se trata de un peligroso virus que se activará dentro de muy pocos días. Generalmente, el supuesto archivo infectado no es un virus sino un archivo del sistema operativo.

- Nunca acepte asesoría no solicitada para desinfectar su computador de algún peligroso virus. Si alguien le advierte que su computador está infectado, actualice su programa Antivirus y realice una revisión de todos los archivos del computador.

- Desconfíe de las Paginas Web desconocidas dónde podrá encontrar software gratuito o promociones de artículos con precios increíblemente bajos.

OPCIONES DE SOFTWARE ANTIVIRUS

Los programas Antivirus detectan los virus mediante una comparación que realiza entre los archivos guardados en el computador y una biblioteca de firmas [8] que identifican a cada Virus. Esto significa que primero se debe conocer el Virus (y por tanto, alguien se debe haber infectado) antes de desarrollar la firma para ese Virus.

Es muy importante mantener actualizada la base de datos de firmas de Virus de su programa antivirus debido a que diariamente aparecen nuevos Virus.

|

ANALIZADORES ANTIVIRUS

|

CALIFICACIÓN

|

COMENTARIOS

|

|

**Symantec Norton Antivirus

2003 9.0**

http://www.symantec.com/region/mx/

| Muy Bueno **

(Shareware 15 días) | Uno de los de mejor desempeño. También es el que tiene la interfaz más clara e intuitiva de los productos probados. No detectó algunos virus de guión ni pudo escanear algunos archivos guardados en las pruebas de zoovirus [9] ** |

| **Panda Antivirus Platinum 7.0**

http://www.pandasoftware.es/ | Bueno *

(Shareware 30 días) | Se integra con el cliente de correo electrónico de Microsoft Outlook y analiza las bases de datos Lotus Notes. No detectó 20 por ciento de los zoovirus [9] polimorfos en las evaluaciones. * |

| **Trend Micro PC-Cillin

2003 10.0**

http://www.trendmicro-la.com/index-e.html | Bueno **

(Shareware 30 días) | Este software ha ganado numerosos premios en publicaciones de prestigio, ha sido retocado para estar al día con las nuevas amenazas de virus, en la época de Internet. Es uno de los programas que ofrece la mejor protección posible para un computador personal. ** |

| **Network Associates

McAfee VirusScan 7.0**

http://es.mcafee.com/ | Pobre *

(Shareware 30 días) | Fuerte análisis de Virus, pero no detectó algunos de los Virus “Salvajes” en el sector de arranque durante análisis totales. Incluye un cortafuegos, así como un análisis de virus para PDAs (Personal Digital Asistant – Asistente Personal Digital). * |

| **Computer associates Etrust

EZ Antivirus 5.4**

http://www.my-etrust.com/TrialReg | Muy Bueno *

(Shareware 30 días) | Tiene una interfaz limpia e intuitiva pero su desempeño deja mucho que desear. No detectó algunas aplicaciones maliciosas ni virus de guión, y tuvo problemas en analizar archivos guardados en pruebas de zoovirus [9]. * |

| **Sophos Anti-Virus**

http://esp.sophos.com/ | Bueno **

(Shareware 30 días) | Protégete contra más de 68.000 virus, troyanos y gusanos. Detecta y elimina virus polimórficos, macros, ubicados en el sector de arranque y los que se trasmiten a través de ejecutables. ** |

| **AVG Anti-Virus System

Free Edition 6.0.404**

http://www.grisoft.com/html/us_downl.htm | Muy Bueno **

(Gratuito) | Potente antivirus gratuito. Permite pausar una revisión en curso para reanudarlo en otro momento. Monitoriza constante del sistema, revisa el correo electrónico, la actualización de la base de datos de virus es gratuita que incluye actualización automática. ** |

| **AntiVir Personal Edition

6.17.03.54**

http://www.free-av.com/ | Muy Bueno **

(Gratuito) | Antivirus potente, eficaz y gratuito. Capaz de detectar y eliminar más de 50.000 virus, incluyendo los de macro y sector de arranque, y es además muy fácil de usar. Vigila en todo momento el sistema con un Virus Guard residente que controla los movimientos de archivos. Incluye un asistente que actualiza automáticamente las bases de datos de virus. ** |

| **Avast! 4.0**

http://www.avast.com/avad1.htm | Bueno **

(Gratuito) | Un antivirus eficaz, eficiente y además gratuito. Capaz de detectar una larga lista de virus, gusanos, troyanos e incluso virus capaces de modificarse a sí mismos. Comprueba la integridad de datos a fin de poder recuperar esos archivos más fácilmente en caso de infección. Incorpora una interfaz para usuarios novatos que no quieren complicarse la vida con demasiadas opciones de configuración. Protege de virus de macros y virus residentes. Se integra con el Explorador de Windows y actualiza la base de datos de virus cada mes. ** |

- Comentarios y calificaciones realizados por la Revista PC World (Jul 2002).

** Comentarios y calificaciones realizados por Softonic (http://www.softonic.com)

REFERENCIAS:

[1] *Cracker*: Aficionado a la computación que disfruta el acceder sin autorización a sistemas informáticos. Su objetivo consiste en vulnerar los sistemas más seguros. Muchos 'Crackers' intentan robar información de los sistemas atacados o destruirla. Los Crackers perjudican a los usuarios de los computadores haciéndoles perder tiempo reparando los daños que causan. Hasta hace solo dos años, la 'Ingeniería Social' era despreciada por los crackers, por no ser un procedimiento técnico. Sin embargo, en los últimos meses ha sido ampliamente utilizada por ellos y se considera un método aceptado, dado que muchos sistemas hubieran sido imposibles de penetrar, sin hacer uso de la 'Ingeniería Social'.

Por el contrario, un Hacker es un Aficionado a los computadores cuya diversión o reto, consiste en aprendérselo todo acerca de un sistema de computación o de una red, y, mediante programación hábil, llevar el sistema al nivel máximo de rendimiento.

**[2] ***Gusano*: Virus informático diseñado para encontrar todos los datos ubicados en la memoria o en un disco duro y alterar lo que encuentre. La alteración puede consistir en cambiar ciertos caracteres por números o intercambiar bytes en la memoria almacenada.

[3] *Troyano*: Programa de computación que aparentemente realiza una función valida pero que contiene, ocultas en su código, instrucciones que provocan daños a los sistemas en que se ejecuta. A diferencia de los virus, los Troyanos no se reproducen a sí mismos; sin embargo, esto no sirve de consuelo para quienes acaban de perder días o semanas de trabajo por su causa.

[4] *Sniffer (husmeador)*: Se trata de un programa que intercepta información que se encuentra en camino a través de Internet y examina cada paquete en busca de información específica, como contraseñas transmitidas en texto sin cifrar.

[5] *Parche*: Reparación rápida en forma de una o más instrucciones agregadas a un programa para corregir errores o mejorar las capacidades del mismo. Programa ejecutable que repara otro programa defectuoso. Reparación de un programa reemplazando una o más líneas de código.

[6] *Extensión*: Sufijo de tres letras (como .bmp (imagen), .php (word), .php (excel), .exe (ejecutable) o .vbs (programa Viusual Basic Script) que se agrega al nombre de los archivos y que generalmente indican su contenido. La extensión se separa del nombre del archivo con un punto.

[7] *Código de Macro:* Consiste en una serie de instrucciones diseñadas para simplificar las tareas repetitivas en programas como Microsoft Word, Excel o Access. Estas instrucciones se ejecutan cuando el archivo asociado a ellas se abre. Muchos Virus infectan estos códigos de Macro y cuando el documento o plantilla que los contiene se abre, el Virus se ejecuta realizando copias de si mismo en otros documentos.

[8] *Biblioteca de Firmas*: Código almacenado que los programas Antivirus identifican como perteneciente a un Virus conocido. Patrón buscado en los archivos para identificar si están infectados por un Virus

[9] *Zoovirus*: Son Virus que solo existen en los laboratorios de las compañías que fabrican software Antivirus y no ha infectado a ningún computador. Son utilizados por los investigadores ya que usan trucos que pueden ser empleados por futuros virus.

*Publicación de este documento en EDUTEKA: Enero 11 de 2003.

Última modificación de este documento: Enero 11 de 2003.*

CRÉDITOS:

Artículo producido por EDUTEKA con información proveniente de:

- Diccionario de Términos de Computación, Bryan Pffenberger, Prentice Hall, 1999.
- Panda Software, Consejos para evitar que los virus afecten a su computador. http://www.pandasoftware.es/virus_info/consejos/default.htm

- Carole Theriault, Introducción a los virus electrónicos, http://esp.sophos.com/virusinfo/whitepapers/videmys.html.

- PC World, Herramientas y reglas para la seguridad en Internet, http://www.pcwla.com.

- Sección [Utilidades / Antivirus / Generales] de Softonic (http://www.softonic.com).