Internet: **www.smu.org.uy**

Epidemia de virus informáticos en la Red

Recientemente se produjo una epidemia de infección por virus de computadoras transmitidos por archivos adjuntos ("attachments") incluidos en mensajes de correo electrónico ("e-mail").

Fueron contaminadas las computadoras de varios usuarios, algunas resultaron inutilizadas y generaron la necesidad de recuperarlas. Aunque esto se haya logrado, a veces a costa de la limpieza de todos los discos y reinstalación de los programas que los usuarios utilizaban con pérdida de datos de archivos personales, estos eventos supusieron para los afectados la necesidad de dedicar tiempo (¿y costo?) perdiendo mientras tanto la posibilidad de realizar con su computadora sus tareas habituales.

Virus informáticos

Son programas de computadora que tienen la particularidad de realizar acciones en una de ellas sin conocimiento y/o autorización del usuario y/o engañándolo respecto a los verdaderos fines de la acción:

– introducirse en ("infectar a") la computadora huésped fundamentalmente vía disquete o correo electrónico;

– autorreproducirse dentro de la misma máquina y/o reenviarse por disquetes o e-mail para infectar otras;

– enviar a computadoras distantes información personal del usuario cuando conecta su máquina a Internet;

– utilizar la máquina infectada conectada a Internet para realizar acciones o ataques en otras computadoras distantes;

– interferir o impedir el funcionamiento normal del equipo y/o eliminar información contenida dentro del mismo.

¿Qué hacer?

Para **reducir el riesgo de penetración** de virus en la computadora y **minimizar el riesgo de que los virus ejecuten** aquellas acciones, conviene:

1. Realizar **respaldos** ("backups", copias de seguridad) periódicas de la información personal (documentos, planillas electrónicas, bases de datos, imágenes, mensajes de correo electrónico, direcciones, etcétera). Pueden hacerse en disquetes, unidades "ZIP", unidades de cinta, grabadoras de CD o en otros discos duros dentro o fuera de la computadora.

2. Tener a disposición un **disquete de arranque** ("boot") del equipo seguramente limpio de virus.

Algunos de los programas antivirus permiten crear los llamados "disquetes de emergencia" o de "rescate" donde se almacena información vital del equipo y que pueden iniciar ("bootear") la computadora y, en ciertos casos, reparar sectores vitales de la misma y eliminar virus infectantes.

3. **Instalar y actualizar periódicamente un sistema antivirus**.

Estos sistemas son capaces de realizar varias tareas en la computadora:

– detectar distintos tipos de virus cuando se los hace examinar (escanear) la memoria y los discos de la computadora;

– detectar "al vuelo" virus en archivos instalados por programas de computación desde disquetes o CDRoms o trasladados a la computadora ("bajados") desde Internet (sitios "Web" y correo electrónico), cuando son ejecutados, abiertos o copiados, permaneciendo vigilantes en segundo plano;

– detectar e impedir acciones habitualmente realizadas por muchos virus ("virus-like activities") aunque no conozcan el/los virus concretos que las producen ("heurística");

– inactivar y eliminar los virus antes de que entren o ya entrados a la computadora y, en muchos casos, rehabilitar los sectores vitales de la

Introducción a Internet para Principiantes

¿Qué es Internet - qué beneficios ofrece - qué equipamiento se necesita?

Las respuestas a estas interrogantes las podrá despejar en este ciclo de charlas.

No se requiere experiencia previa.
Inscripciones gratuitas en Sección Socios
Cupos limitados – 4 grupos a elección los días:

28 de noviembre
5 de diciembre
12 de diciembre
19 de diciembre

17:00 horas. Local del SMU, Br. Artigas 1521

Organiza: Comisión de Telemática del SMU, apoya Chasque.

máquina y los archivos contaminado o alterados por ellos.

Debe **actualizarse ("update")** frecuentemente (días-semanal) la **base de datos de definiciones de los virus conocidos por el antivirus** con información sobre ejemplares nuevos (o nuevas versiones), que los programas ponen a disposición de los usuarios, con una frecuencia que depende de la aparición de aquellos (ocurre a veces en días, otras en una o dos semanas). En algunos programas se les denomina Live Update (actualización en vivo): se transfiere la nueva información y se la instala en la computadora conectada a Internet, en escaso tiempo y sin acciones especiales por parte del usuario.

Debe **actualizarse periódicamente el propio programa antivirus**, cosa que algunos realizan en el momento en que hacen alguna actualización de las definiciones de virus. Incorpora ajustes en su funcionamiento.

Es muy conveniente conseguir las **nuevas versiones ("upgrade")** del antivirus, probablemente anuales, donde se incorporan importantes mejoras en su funcionalidad.

Entre los más conocidos y recomendados (existen 30 o más antivirus en el mercado) están (orden alfabético):

- AVP (Kaspersky Antiviral Toolkit Pro) - http://www.avp.ch/
- NAI VirusScan (McAfee-Solomon) - http://www.nai.com/
- Norton Antivirus - http://www.symantec.com/
- Panda Platinum Antivirus - http://www.pandasoftware.com/

Computer Associates (http://antivirus.cai.com) ofrece InoculateIT en forma gratuita para uso personal.

Hay otros programas especializados en la detección y eliminación de un tipo especial de virus de computadora (y que "conocen" muchos más que los antivirus "de amplio espectro"), los **troyanos** (que, llegados en adjuntos de e-mail, introducen en aquélla programas que la transforman en un "servidor" que envía información hacia afuera cuando está conectada a Internet). El más conocido es The Cleaner (http://www.moosoft.com).

4. **Instalar algún sistema de protección contra intromisiones** (acciones de "hackers") **desde Internet** ("firewall", "pantalla de fuego").

* Symantec ofrece Norton Internet Security en (http://security2.norton.com/common/1033/sym/sym_recommends.asp?go=NIS).
* ZoneLabs (http://www.zonelabs.com) ofrece el ZoneAlarm, un sistema de protección sencillo, muy efectivo y gratuito para computadoras de uso personal.

5. Sin embargo, una **parte sustancial de la protección** de nuestra computadora es **nuestra propia conducta (y la de nuestros familiares que también la utilicen).**

Por ello es aconsejable:

Nunca abrir (ejecutar, darle doble clic con el botón izquierdo del mouse (puede depender del programa de correo electrónico en uso en la computadora) **archivos adjuntos a un e-mail sin escanearlos** (al mensaje concreto, no necesariamente todo un disco) con el antivirus (el procedimiento puede depender del antivirus utilizado). En algunos programas antivirus que realizan en la computadora la **vigilancia en segundo plano**, es suficiente con **copiar** el archivo adjunto a un directorio (carpeta) del disco (determinado/a por el usuario) pues será escaneado en el momento de la copia y detectará virus si están entre sus definiciones conocidas (por eso la perentoria necesidad de la actualización periódica) o mediante su heurística. En este caso el virus será detectado y podrá eliminarse el mensaje portador antes de que se ejecute e infecte la computadora.

Téngase en cuenta que el mensaje puede provenir de la computadora de una persona conocida, incluso un compañero bien conocido: su computadora puede estar infectada sin que él lo sepa y el virus se siembra desde ella hacia otras. Los usuarios de la red smu-a comprobaron por sí mismos este fenómeno en esta epidemia reciente. En esta materia la mejor conducta es la de **"ser desconfiado", siempre, con lo que llega** proveniente de un desconocido o de un conocido...

Otros aspectos

1. **Nunca** reenviar en forma indiscriminada mensajes de alertas sobre virus.

En general estos mensajes se reconocen por las siguientes características:

a) Alertan sobre la circulación de "virus" que producirán catástrofes apocalípticas ("les destruirán todos los archivos de la computadora..."). b) Citan a reconocidas empresas informáticas como supuestas fuentes de la información (Microsoft, AOL, IBM, etcétera). c) y, **fundamentalmente,** incitan a distribuir el alerta a todos sus conocidos.

La abrumadora mayoría de los "virus" sobre los que se alerta son **falsos ("hoaxes")** (no son virus, no existen). Estos "alertas" reverberan incesantemente en las redes informáticas produciendo enorme sobrecarga de los servidores de correo electrónico.

Y, detrás de ellas, subyace la **"captura" de direcciones de correo electrónico** que luego son comercializadas para el envío de e-mails no deseados ("spam") a los integrantes de las libretas de direcciones de los bien intencionados incautos que, en definitiva, las expusieron a la vista de todo el mundo.

En caso de dudas consulte previamente.

Tenga en cuenta que la mayoría de los virus sobre los cuales se alerta, hace semanas o meses que están contenidos en las definiciones de los antivirus y quien tenga el suyo correctamente actualizado no será infectado, en caso de que se trate de un virus real. De modo que no hay tal apuro... y ningún alerta de estos supera las consideraciones hechas en el 'conviene' de "¿Qué hacer?", más arriba.

El virus MTX (aparecido a fines de agosto de 2000) que protagonizó la epidemia reciente de nuestra red con infecciones hasta bien adentrado el mes de octubre, estaba contenido en la base de datos de alguno de los antivirus citados más arriba ¡desde el 3 de setiembre de 2000!

2. **Nunca** responder a e-mails que no estén dirigidos a usted, especialmente aquellos que informan que para dejar de recibir esos mensajes deben responder a tal dirección. Esta respuesta o su protesta, incluso, significan para los enviantes que la dirección en cuestión está "viva" y en uso. Tirar verde para recoger maduro...

3. **Nunca** utilizar la dirección privada cuando sea solicitada en algún **sitio de Internet que no merezca plena confianza y del cual uno desea realmente recibir mensajes**. Se puede obtener una cuenta web mail gratuita para esos fines. (www.hotmail.com es una buena alternativa).

4. **Utilizar contraseñas** que combinen números y letras hasta 7 u 8 caracteres y cambiarlas con frecuencia.

5. **Actualizar el navegador de Internet y el programa de correo electrónico** (www.microsoft.com, www.netscape.com) u otro.

6. **Verificar**, antes de enviar su número de tarjeta de crédito, que se trate de un **sitio seguro**, en el navegador de Internet debe aparecer el ícono de candado cerrado o el ícono de la llave.

AP Alejandro Juan
Coordinador de la Red Médica
con la colaboración del Dr. Ricardo Caritat