Por Roxana Bassi rox@roxanabassi.com.ar / http://www.roxanabassi.com.ar

Publicado en la sección “los cuadernos de Internet World” en la revista Internet World Latinoamérica en el período 1995-1999

Curso Número 6

Mitos y verdades sobre la Seguridad al conectarse a la Red

Hasta hace muy poco tiempo, la mayoría de las computadoras personales eran entidades aisladas tanto en las empresas como en el hogar. Con el advenimiento de la Internet y las redes, comienzan a surgir preocupaciones por los peligros de la interconexión: los accesos indeseados y otras amenazas externas, como los virus.

En esta entrega se analizan algunas de dichas amenazas así como los mitos existentes sobre la seguridad y, además, se presentan las técnicas básicas para evitar problemas. El objetivo es claro: aprender a proteger la información que se genera y almacena en una computadora ya que tiene un singular valor para todo usuario.

Las medidas de protección son muy distintas si uno posee una computadora del tipo *servidor*.

Los virus

¿Qué son?

Los virus son pequeños programas de computadora que tienen la capacidad de autoduplicarse y *parasitar* a otros programas. Una vez que se difunden, los

virus se activan bajo determinadas circunstancias y, en general provocan algún daño o molestia.

Mito: Se pueden difundir peligrosos virus por e-mail que destruyan todo su disco rígido. Si recibe un mail con un virus, bórrelo sin siquiera leer el mensaje. Existe un mito muy popular sobre un famoso virus llamado *Penpal Grettings* o *Good Times.* Se trata de un mensaje que asegura que de recibir un e-mail con alguno de estos *subjects* (temas) debe ser borrado inmediatamente sin leerlo, o de lo contrario nos contagiará con un virus.

Verdad: No hay ninguna forma de que un virus se contagie con la simple acción de leer un mensaje de texto de correo electrónico, aunque si hay formas de contagiarse por Internet (ver más adelante).

[pantalla 1: Good Times]

¿Dónde se alojan?

Dado que un virus es un programa, sólo puede infectar a otros programas. Esto significa que los archivos de datos (como una foto, una carta o una planilla) no pueden contener virus, con la excepción de los nuevos *macro virus*.

Los virus están inactivos hasta que son ejecutados (o mejor dicho, hasta que el programa donde se alojan es ejecutado, corrido). A partir de ese momento pueden tomar control de su máquina, quedarse "residentes" en la memoria y dedicarse a contagiar y causar daño.

Los *macro virus* son unos modernos virus que infectan documentos de Word o planillas Excel, que si bien son archivos de datos pueden contener también

órdenes programadas por el usuario llamadas macros, donde el virus puede alojarse.

¿Qué hacen?

Algunos virus son inocentes y no causan daño. Pero otros están preparados para activarse en determinadas circunstancias (ej. una fecha, una hora) y ejecutar alguna actividad maligna, desde reemplazar todos los "9" por "6" en una planilla de cálculo hasta destruir por completo su disco rígido.

¿Quién los crea?

Los virus son creados por expertos programadores. Su estrategia de propagación y daño demandan un excelente conocimiento de los lenguajes de programación y los sistemas operativos. Muchas personas se dedican a crear virus para pasar el tiempo, para molestar, o hasta como elemento de venganza o simplemente de diversión personal.

¿Cómo se distribuyen?

Los virus se distribuyen al copiar archivos de computadora en computadora, donde -inadvertidamente- también se copia al virus. Esto puede suceder tanto al llevar un *diskette* del trabajo a casa, por duplicación ilegal de software, como al bajar algún archivo de Internet, entre otras razones.

Caballos de Troya

Los virus llamados *Caballos de Troya*. se difunden *disfrazados* como un supuesto programa útil. Por ejemplo, usted puede recibir una nueva versión de su compactador favorito, que en realidad no es tal sino que se trata de un virus

que se hace pasar por un programa útil para que usted lo ejecute. Para evitar ser engañado con estos virus, desconfíe de nuevas versiones *mejoradas* de los programas que no provengan del sitio oficial de la compañía que lo genera.

Formas de contagio

Las únicas formas de que un virus ingrese en nuestro sistema a través de Internet son:

1) Al ejecutarse manualmente un programa bajado de la Internet, sin previamente verificarlo contra Virus. Esto puede suceder de varias formas:

a) Al bajarse un archivo cualquiera vía Web o FTP (un software, una demostración, un *plug-in* para el navegador). Muchos sitios FTP de donde se pueden obtener archivos garantizan que sus programas están libres de virus, sin embargo, esto no siempre es así.

b) Si le llega un archivo ejecutable infectado como un *attach* (adosado) de un e-mail y se lo ejecuta sin verificarlo previamente con un antivirus. Es la forma más común de difusión de los llamados Macro virus, que pueden acompañar a las cartas de Word o planillas de Excel.

2) Al ejecutarse en forma automática algún programa infectado de la Internet.

Esto es especialmente peligroso. Los *plug-ins* (agregados) que usted coloca en su navegador están capacitados para ejecutar automáticamente los archivos que reciben. Por ejemplo, si usted coloca un agregado para ver películas en formato MPEG, cuando baje la película, el agregado correrá automáticamente el video. Para aumentar su seguridad, minimice el uso de agregados y verifique todo archivo que baja de Internet antes de ejecutarlo.

Historia del Gusano de Internet

Un *Worm* (gusano) es un programa similar al virus, pero que a diferencia de éste no requiere infectar a otro programa, ya que se difunde en forma autónoma de computadora a computadora.

En Noviembre de 1988 un estudiante norteamericano de la Universidad de Cornell, llamado Robert Morris, descubrió un pequeño error en el programa más utilizado para rutear e-mails *(sendmail)* por toda la Internet. Robert diseñó entonces un *Worm* que se copiaba de servidor en servidor, burlando la seguridad aprovechándose de este error. El Gusano se distribuyó por Internet en pocas horas, causando caos en la mayoría de los grandes sistemas y dejando inactivos los centros de cómputos de la mayoría de las universidades y los centros del Gobierno de los Estados Unidos. Dos días después comenzó a repararse el daño que costó millones de dólares y demostró cuán frágil era la seguridad de los sistemas en ese entonces.

¿Cómo protegerse?

Un antivirus es un programa diseñado para detectar la infección de virus en otros programas. Existen muchas formas de antivirus, pero la más usual es la que contiene un registro de identificación de todos los virus conocidos (llamada *signature)* y que busca su computadora comparando todo archivo contra estos registros.

La mejor prevención es tener un antivirus activo constantemente y chequear todo archivo y mensaje que llegue del exterior.

Existen dos antivirus muy utilizados que pueden ser obtenidos para prueba por un período limitado. Obtenga la versión adecuada para su sistema operativo.
El Scan Antivirus de McAfee en **http://www.mcafee.com/prod/av/av.html**
El Thunderbyte Antivirus en **http://www.thunderbyte.com/new_users.html**

Recuerde que debido a la gran cantidad de virus nuevos no sirve de nada tener un antivirus con varios meses de antigüedad. Actualice sus versiones regularmente.

¿Cómo proteger a otros?

Básicamente, si su sistema está libre de virus usted no representará ninguna amenaza para el resto de los *cybernautas.*

Y por favor, si recibe un mensaje sobre un virus por e-mail, verifique su autenticidad antes de reenviarlo a todos sus conocidos de la Red. Es una fórmula para detener -entre todos- este tipo de falsos rumores.

Accesos externos

Mito: desde que usted se conecta a Internet se expone a que un vándalo informático invada su PC y le borre todo sus disco rígido, o peor aun, le robe información privada.
Verdad: su computadora jamas podrá ser accedida desde el exterior, a menos que se trate de un *server*.

Básicamente existen dos clases de computadoras en Internet, sin importar sus marcas ni modelos:

- Los llamados *servers* (servidores) son computadoras que ofrecen información al mundo y por lo tanto deben estar encendidas y conectadas a Internet las 24 horas del día mediante conexiones dedicadas.
- Los llamados *clients* (clientes), computadoras que se conectan a Internet cada vez que se desee consultar algo o intercambiar información, pero que no ofrecen datos a los navegantes externos.

Un computadora *server* está preparada para recibir pedidos externos de los navegantes y por lo tanto puede ser invadida por un *cracker*.
Una computadora que es sólo *cliente* no ofrece a ningún visitante externo la posibilidad de invadirla. Por lo tanto, no debe temer que nadie ingrese en su computadora y le robe datos, ya que es imposible.

Sin embargo, existen ciertos riesgos mínimos de que algunos programas automáticos se instalen en las computadoras y envíen al exterior datos sobre

nosotros (como dirección de e-mail, sitios Web mas visitados, claves de acceso a sitios, etc.)

Cookies

Las *cookies* (galletas) son pequeños archivos con datos que algunos sitios Web depositan en forma automática en las computadoras. Lo hacen con el objetivo de almacenar allí información sobre las persona y sus preferencias. Por ejemplo, la primera vez que visite un site y complete algún formulario con sus datos y perfil, el sistema podrá enviarle una *cookie* con una identificación de quién es. La siguiente vez que retorne allí, el sitio Web pedirá automáticamente a su computadora la *cookie*, y a través de ella lo reconocerá.

Las *cookies* en si mismas no representan ningún peligro a la seguridad del sistema, aunque son consideradas por muchas personas como una invasión a la privacidad al obtener, almacenar y enviar datos sin autorización. Si la idea de las *cookies* le molesta, lo mejor es optar por recibir un aviso antes de enviarlas, activando la opción correspondiente en el menú de su navegador.

[pantalla 2: Cookie]

Java, Javascript y ActiveX

El lenguaje Java de programación es una variante del C++ creada por la empresa Sun Microsystems. El Javascript es una versión de *scripting*. El objetivo de ambos es brindar mayor interactividad y personalización a los Web sites.

El entorno Activex es una tecnología similar creada con los mismos objetivos por la empresa Microsoft.

Sin embargo, a veces fallan en su objetivo de brindar entornos seguros de trabajo, tal como puede observarse visitando los *applets* hostiles de **http://www.math.gatech.edu/~mladue/HostileApplets.html**

Si la idea del Java y Activex lo inquieta, lo mejor es deshabilitar el soporte para ellos en el menú correspondiente de su navegador. Sin embargo, recuerde que si lo hace, también perderá las posibilidades de animaciones e interactividad que le brindan estos lenguajes.

Consejos de Seguridad para su Navegador

Su navegador le permite elegir que tipo de advertencias de seguridad desea recibir mientras explora la Web.

Microsoft Explorer V 3.0

Para cambiar los niveles de seguridad, en el nivel **Ver (View)** haga click en **Opciones (Options)**. Haga click en la ficha **Avanzado** (**Advanced**).

En la ficha A**dvertencias** (**Warnings**) active:

1. La primera casilla si desea que se le avise cada vez que envíe información aun sitio no seguro de la Internet.
2. La segunda casilla si desea un aviso cuando usted se desplaza de un sitio seguro a otro que no lo es
3. La tercera casilla si desea que se le avise cuando al seguridad de un sitio sea cuestionable.

4. La cuarta casilla si desea ser advertido cada vez que un sitio intente enviar o recibir una *cookie*.

En la ficha **Seguridad**:

Bajo **Contenido Activo** usted puede controlar que cosas su PC puede ejecutar automáticamente.

- En **Nivel de seguridad**, elija el que se adecue a su nivel de usuario.
- **Permitir programas Java**: indique si desea que estos programas pueden correr automáticamente.
- Elija el nivel de aviso ante controles ActiveX.

[Pantalla 3 Explorer]

Netscape Navigator 3.0

Bajo **Options (Opciones)** elija **Security (Seguridad)**

En la ficha **General** elija:

1. La primera casilla si desea que el sistema le avise cuando ingrese a un sitio seguro.
2. La segunda casilla si desea un aviso cuando se desplaza de un sitio seguro a otro que no lo es.
3. La tercera casilla si desea que se le avise cuando al seguridad de un sitio sea cuestionable.
4. La cuarta casilla si desea que se le avise cada vez que envíe información aun sitio no seguro de la Internet.

Bajo **Options (Opciones)** elija **Network Preferences (preferencias de red)** y luego **Preferences (Preferencias).**

En la ficha **Protocols (Protocolos)** seleccione**:**

- **Accepting a Cookie** si desea ser advertido antes de aceptar información de una Cookie.
- **Submitting a form by e-mail** si desea ser advertido antes de enviar datos inseguros por correo.

[Pantalla 4: Navigator]

Las Claves secretas (passwords)

Mito: las claves de acceso son innecesarias. Elija una palabra sencilla, como su nombre y podrá recordarla fácilmente.

Verdad: las palabras claves son mecanismos básicos de protección. Si sus datos o sus recursos no son valiosos, no se moleste en utilizarlas. Pero si usted considera que posee alguna información de importancia, es una buena idea observar los siguientes consejos sobre cómo elegir una clave.

Usted seguramente utiliza una o varias claves secretas para acceder a Internet, proteger sus archivos privados, etc.

Hay algunos consejos sobre cómo debe elegirse una clave.

Lo que Nunca debe usarse como Clave

- Cualquier palabra o número fácilmente relacionado con uno mismo (es lo primero que buscan los *hackers*): nombre, apodo de la primaria, numero de documento, patente del auto, fecha de nacimiento, nombre de un hijo, calle donde vive, etc.
- Cualquier letra repetida varias veces, como por ejemplo *zzzzzzz* o *777777*
- Cualquier escalera normal, como por ejemplo *1234*, *abcdef*, *doremifasol*
- Palabras usuales como: Clave, MiClave, TopSecret, Secreto, etc.
- Ninguna variante de todo lo anterior escrito al revés.

Además:

- Nunca usar la misma clave en varios lugares (si alguien averigua una, nada impedirá que acceda al resto de los servicios protegidas con la misma clave).
- No escribirla en ninguna parte en la medida de los posible (nunca en su agenda o billetera).
- No compartirla con nadie y, si debe hacerlo (por ejemplo, cuando se va de vacaciones), cámbiela en cuanto pueda.
- No almacenarla en un archivo en su disco rígido.

Lo que sí se puede usar como clave

- Dos palabras al azar separadas de un signo raro, como *xilofon$rayos-x* (elíjalas de un diccionario abriendo páginas al azar).
- Una palabra inventada: *aluminatividad.*
- Una cadena de caracteres al azar: *YU6790HGJ*
- Una frase clave (*pass phrase*). En lugar de tipear la frase completa, que sería muy molesto, utilice sólo la primera letra de cada palabra. Por ejemplo, si la frase fuera *"En casa de herrero cuchillo de palo",* la clave de acceso seria *ecdhcdp* , una cadena de caracteres difícil de recordar sin la frase.

¡Nunca envíe su clave de acceso a Internet por e-mail !

Uno de los trucos más usados para robar claves de acceso es enviar un mail al usuario como si se tratara de un mensaje originado por el proveedor de servicios. El mail podrá decir algo inocente como *"envíe su clave por correo para verificar si su cuenta de Internet funciona correctamente"*. Si usted comete el error de responder al mensaje, que seguramente esté dirigido a una

cuenta de correo falsa, puede que al mes siguiente note un aumento en sus horas de consumo de Internet.

Jamás debe enviar ninguna clave de acceso por e-mail. Su proveedor (si realmente se trata de él) posee mecanismos válidos para verificarla sin necesidad de preguntársela.

Encriptación de datos

Mito: El correo electrónico es absolutamente seguro. A través suyo puede enviarse la información más valiosa por el sin correr riesgos, ya que jamás puede ser interceptado o leído.
Verdad: Si bien es poco probable, su e-mail puede ser interceptado y leído. Si usted envía información importante por correo (como ser información de su empresa o productos, estudios de mercado o información estratégica) le conviene conocer y utilizar los mecanismos de encriptación existentes.

Cuando hablamos de encriptación de datos, en general asociamos el concepto con las películas de espías y secretos de estado, donde se manejaban códigos para proteger las cartas enviadas entre miembros del mismo bando.
Estas ideas no podemos sentirlas más alejadas de nuestra realidad. Sin embargo, la encriptación de datos era cada vez más y más necesaria con Internet convirtiéndose en un medio mundial de comunicación.

Supongamos que yo quiera enviarle un mensaje pero no quiera que nadie excepto usted pueda leerlo. Yo podría encriptar o cifrar ese mensaje, es decir, mezclarlo de una forma complicada de modo que sólo alguien que sabe cómo lo hice pueda deshacer los pasos y volver al mensaje original.

Un *criptosistema* es un conjunto de reglas que determina cómo se codifican (mezclan) y decodifican (des-mezclan) los datos para volver al texto original.

Existen varios tipos de *criptosistemas*, que pueden no utilizar claves, utilizar una clave o más de una.

Una clave es un conjunto (patrón) de símbolos *(bits)* usados para codificar o decodificar un mensaje. La clave suele derivarse de una contraseña *(password)* o de una frase clave *(pass phrase).*

En este caso, yo utilizaría una clave *(key)* criptográfica para encriptar el mensaje, y usted usaría la misma clave para descifrarlo o desencriptarlo. Esto es lo que llamamos un sistema criptografico de llave única *(single key),* ya que ambos utilizamos el mismo código para *cerrar* y para *abrir* el mensaje.

Un sistema tradicional de encriptación como éste implica que la clave única debe haber sido intercambiada *primero* entre las dos personas que deseen enviarse documentos encriptados. Es decir, yo debería haber s28le contado a usted que la clave para decodificar mi carta es *sdhgfhgdsf.* Esto implica que antes debería haber enviado la clave por un medio seguro: un fax, un *courier*, un sobre. Este es el principal problema: ¿cómo lograr intercambiar esas llaves con absoluta seguridad? No sólo eso, sino que personas extrañas no podrían intercambiarse archivos sin antes poder enviarse la clave de acceso (imagínese la importancia que esto tiene para el comercio electrónico).

[gráfico de sistemas de una clave]

Existen varios sistemas de una clave muy utilizados, sin embargo, a continuación se analiza un método aun más seguro de protección de datos.

Los Sistemas de clave pública y clave privada

Imagínese que usted tiene una caja de seguridad. Encarga a su cerrajero dos tipos de llave para la cerradura: una única llave *(clave privada)* que puede abrir la caja y varias llaves *(claves públicas)* que pueden cerrarla, pero NO abrirla. Cualquier persona con la llave que cierra *(clave pública)* puede dejar un mensaje dentro de la caja que sólo usted podrá abrir.

¿Cuál sería el riesgo de entregar a todos una copia de nuestra llave que cierra?

En un sistema de *clave pública* (también llamados algoritmos D-H) usted tiene dos claves. Una clave, la llamada pública, puede ser distribuida libremente y cualquier persona que quiera enviarle un mensaje codificado podrá usar su clave pública para la codificación.

La otra clave, la *privada*, se conserva secreta y se usa sólo para la desencriptación. De la clave pública no puede deducirse la privada.

La clave pública puede ser distribuida libremente a través de la red (usualmente se la agrega al final de un mensaje, donde se ven como cuatro o cinco líneas de caracteres mezclados).

Cualquier persona, incluso un desconocidevauth2o, puede usar su clave pública para enviarle un mensaje cifrado, el cual sólo podrá ser descifrado por usted (ni siquiera quien la encriptó originalmente puede revertir el proceso).

Los sistemas de *clave pública* fueron inventados en 1976 por Whitfield Diffie y Martin Hellman.

[gráfico de sistemas de dos claves]

Autenticación o firma electrónica

Otra razón para el uso de las claves públicas es la autenticación: poder garantizar que un mensaje proviene efectivamente de una persona en particular y que no fue alterado en el medio (imagínese el caso de una orden de compra o de un pago electrónico).

La clave privada de quien lo envió puede ser usada para encriptar o firmar un mensaje, de este modo garantizando la autoría del mensaje. Para generar una *firma"* el programa de encriptación usa una función llamada *hashing* que logra una serie de *bits* resultantes de modo tal que, si el mensaje fuera alterado, el resultado de aplicar este proceso sería muy distinto. Luego se usa la clave privada para formar la firma.

El PGP (Pretty Good Privacy)

Es un software de criptografia de alta seguridad existente para la mayoría de los sistemas operativos (PC DOS, Unix, VAX/VMS, Macintosh y Amiga, entre otros). Creado por Phil Zimmerman, uno de lo héroes de Internet, ya que corre riesgo de ir a la cárcel por haber hecho público un algoritmo de encriptación secreto.

Es un algoritmo de clave pública, descripto en la sección anterior, que permite que las personas intercambien mensajes con privacidad, autenticación y conveniencia.

- Privacidad porque sólo aquellos para los cuales estaba destinado un mensaje pueden recibirlo.
- Autenticación porque puede verificarse que un mensaje público publicado por una determinada persona haya podido ser escrito sólo por ella (esto es lo que se llama firma electrónica).

- Conveniencia porque la privacidad y la autenticación se pueden obtener sin los problemas de manejar claves que se tienen en general con el software común de criptografia. No se requiere un canal seguro para intercambiar claves entre usuarios.

Puede obtener el PGP versión shareware en **http://www.pgp.com**

Esto ha sido solamente una introducción conceptual a la protección criptografica de datos. En otra edición de los archivos veremos en detalle como utilizar el PGP.

¡Queremos que nos escriba!

Quienes hacemos los *"Archivos de Internet World"* queremos saber su opinión. Por favor escríbanos a **archivo@iworld.com.ar** contándonos sus sugerencias y qué temas le gustaría ver cubiertos en próximas ediciones. ¡Gracias!