Nociones básicas de seguridad para nuevos usuarios de computadoras

Jornadas de Introducción a la Computación
C.S.A. La Trama

Quique
e-mail: quique@sindominio.net

Zaragoza, 5 de Mayo de 2002

Resumen

Este artículo pretende explicar de forma clara que medidas preventivas conviene tomar a la hora de usar Internet, para evitar contagios de virus y otros problemas de seguridad.

Índice

1. Sobre este documento

La versión más reciente de este documento se encuentra en
`http://sindominio.net/ayuda`

2. Know your enemy

Desde que el célebre gusano que colapsó la red de ArpaNet en los tiempos de María Castaña (cuando reinaba el Rey Carolo y el pimiento era colorao), ha ido naciendo una sucesión de gusanos, troyanos y virus, que han causado incalculables daños. Algunos de ellos han alcanzado notoria fama, como el clásico "Viernes 13" o el reciente "I love you". Con el tiempo, la mayoría de los usuarios han terminado asumiendo la existencia de los virus informáticos como algo inevitable e inherente a las computadoras. Sin embargo esto no es cierto. Basta seguir unos mínimos principios de seguridad para mantener nuestro sistema inmune a este peligro.

2.1. Sistemas resistentes y sistemas enfermizos

Echemos un vistazo a los principales sistemas operativos:

GNU/Linux, Mac OS X, *BSD y otros sistemas tipo UNIX En sus más de 30 años de historia apenas se han conocido unos pocos gusanos y troyanos. Dada las características de seguridad de los sistemas tipo Unix, para que estos programillas fueran realmente dañinos deberían ser ejecutados por el usuario root.

MacOS (hasta la versión 9) Los macintosh son ordenadores relativamente seguros en lo que a sufrir virus se refiere. Los pocos que se han escrito son relativamente inofensivos. Aún así es recomendable disponer de un antivirus como Desinfectant o SAM para asegurarse de no contagiarse con algún virus que pueda quedar latente por ahí. Nota: sin embargo los mac son sensibles a los virus tipo Macro, que luego veremos.

MS Windows El sistema predominante en el mercado se caracteriza precisamente por su inseguridad. Se le han encontrado multitud de agujeros, y hay literalmente miles de virus que lo atacan. Algunos de ellos causan daños irreparables: formateo del disco duro o incluso infección del BIOS, arruinando en ocasiones la placa base y

obligando a comprar una nueva. Así pues, la primera conclusión para evitar sufrir los estragos de los virus sería no usar Microsoft Windows como sistema operativo. Si lo usamos, es muy recomandable instalar un antivirus y cumplir seriamente unas medidas mínimas de protección.

2.2. Tipos de programas dañinos

Troyano o caballo de Troya Es un programa aparentemente útil, pero que al usarlo hace otras cosas sin que lo sepamos: desproteger el sistema para facilitar el acceso desde el exterior, borrar ficheros, etc.

Spyware Es un tipo de troyano. No causa daños en nuestro sistema, pero al usarlo, además de lo que le vemos hacer, envía información sobre ti: las páginas web que visitas, la música que escuchas, etc.

Gusano Es un programa que utiliza las redes de comunicaciones para expandirse de sistema en sistema. No causan daños directamente, sino debido a su multiplicación, que puede llegar a extremos de colapsar una red.

Hoax (bulo) Es un gusano manual ;-) Son mensajes de correo advirtiendo de supuestos virus peligrosos y pidiendo que avises a todos tus conocidos. Suelen ser muy catastrofistas ("si lees un mensaje llamado Good Times se borrará toda la información de su disco duro y no la podrás recuperar") y nombrar a alguna empresa de prestigio (IBM, Microsoft, etc), pero no incluyen ni fecha ni ninguna manera de comprobar el aviso.

Virus Es un programa diseñado para autorreplicarse y ejecutar acciones no deseadas dentro del ordenador. Según de que tipo sean pueden infectar documentos y programas o los sectores de arranque de los discos. Últimamente procuran distribuirse vía internet, para expandirse lo más rápidamente posible.

Virus de tipo macro La suite ofimática Microsoft Office incluye la posibilidad de crear macros (atajos) en Visual Basic. El problema es que la falta de seguridad de MS Office posibilita que estas macros puedan hacer demasiadas cosas (prácticamente de todo), tanto útiles como malignas.

2.3. Outlook: puerta abierta a los virus

Hemos visto como Windows es el sistema operativo más susceptible de ser infectado por un virus, y como éstos se expanden con frecuencia vía e-mail.

Sin embargo Outlook y Outlook Express, los clientes de correo de Microsoft, presentan numerosos problemas de seguridad. De hecho, la mayoría de los virus que se transmiten por correo electrónico afectan únicamente a estos programas, aprovechando vulnerabilidades que les hacen ejecutar automáticamente el código adjuntado a un mensaje al leerlo (¡o incluso sin leerlo, simplemente al recibirlo!).

En definitiva es sumamente desaconsejable usar Outlook, pues puede causarnos muy desagradables sorpresas.

Otro problema que no sólo afecta a Outlook, sino también a algunos otros clientes de correo,son los mensajes en HTML. Estos mensajes pueden contener código JavaScript malicioso.

2.4. Microsoft Office y los virus de tipo Macro

Un virus tipo macro puede infectar tu copia de Office para incluirse en todos los documentos que abras. Así pues es sumamente recomendable no usar MS Office, sino otras suites, como Open Office (`http://www.openoffice.org`), que es software libre.

2.5. MS Internet Explorer y MS Internet Information Server

Tras el correo electrónico y los documentos de Office, el tercer método favorito de propagación de los virus actuales es a través de la web.

Una vez más, el navegador de Microsoft es especialmente inseguro. Microsoft se ve obligada a publicar parches de seguridad tan frecuentemente que resulta prácticamente imposible mantener el navegador actualizado. Lo más recomendable usar otros navegadores.

Un ordenador doméstico no tendrá generalmente instalado IIS, el servidor web de Microsoft. Las "extensiones de FrontPage" y otras vulnerabilidades nunca bien corregidas hacen de este programa otro queso gruyère. Si necesitamos un servidor web, Apache es más seguro, más eficiente y es software libre.

3. Medidas de prevención contra los virus

- Siempre que sea posible, utiliza software libre en vez de software propietario. La experiencia demuestra que el software libre es mucho menos propenso a tener agujeros de seguridad que el propietario. Además es difícil saber si un programa propietario es spyware, pues su código fuente no está disponible.

- Si utilizas Windows, desactiva la *feature* Windows Scripting Host. Tienes instrucciones (en inglés) en:
  `http://www.sophos.com/support/faqs/wsh.html`
  `http://www.datafellows.com/virus-info/u-vbs/uninstall-vbs.html`
  `http://www.symantec.com/avcenter/venc/data/win.script.hosting.html`
  Una vez hecho esto no podrás usar scripts de VBS, pero la mayoría de los usuarios no usan scripts de VBS para nada.

- No instales programas obtenidos de fuentes no fiables. Esto incluye los programas en java incluídos en algunas páginas web, que te pasen por IRC (chat), etc.

- No uses el programa Outlook para leer tu correo. Si usas Windows, puedes usar el lector de Correo de Mozilla. En Internet hay muchos programas de correo disponibles, gratuitos (Eudora Light, Pegasus, Netscape Messenger...) o *shareware* (The Bat!, Kaufman Mail Warrior...). Un buen programa para el Mac OS clásico es Musashi. En sistemas tipo Unix los más apreciados son Sylpheed y Mutt.

- Si recibes un e-mail con un fichero adjunto de alguien que no conoces, no abras el fichero. Si proviene de alguien conocido, no lo abras si en el cuerpo del mensaje no dice de que se trata.

- Nunca ejecutes programas recibidos por correo electrónico, aunque provengan de alguien conocido. A veces, los virus se ocultan bajo salvapantallas o jueguecitos aparentemente inocentes.

- Si tu programa de correo puede ver mensajes en HTML y soporta JavaScript, desactiva el JavaScript en las preferencias.
  Lo más recomendable es no leer ni escribir mensajes en HTML, sino en ASCII (texto puro, sin colores, tamaños, negritas, etc). Si alguien te envía mensajes en HTML, aconséjale que deje de hacerlo. Además de más seguros, los mensajes en ASCII son más pequeños y se descargan más rápido.

- No uses MS Office, sino otras suites ofimáticas como OpenOffice.

- Si por alguna razón necesitas usar MS Office:

  - no aceptes documentos en formato .doc. Pídele a la persona que te lo ha hecho llegar que te lo pase en otro formato, como RTF (formato de intercambio o texto enriquecido). Véase el documento *Porqué no usar el formato de Microsoft Word (.doc)*
  - cuando abras documentos realizados por otras personas, no aceptes las macros que puedan contener.

- No uses el navegador Internet Explorer, sino otros como Mozilla (que es software libre), Netscape 6 u Opera.

- Instala un antivirus en tu computadora y mantenlo actualizado.

- Desconfía de los avisos de virus que te lleguen por correo electrónico, especialmente si solicitan que envíes ese aviso a otras personas. Si no incluyen una fuente de información comprobable, lo más probable es que sean un bulo (*hoax*). Si recibes un aviso de este tipo, comprueba que no sea un *hoax* en:
  `http://www.sophos.com/virusinfo/scares/`
  `http://www.symantec.com/avcenter/hoax.html`
  `http://www.datafellows.com/virus-info/hoax/`
  `http://hoaxbusters.ciac.org/`

- Si la computadora la usan otras personas, también deben seguir estas medidas.

4. Consejos generales de seguridad

- Utiliza contraseñas fuertes, y protégelas. Véase el apartado 5.
- Haz copias de seguridad de tus documentos (en CD-ROM, diskette, en otro ordenador...). Los discos duros también se rompen.
- Las nuevas versiones de los programas no sólo incluyen nuevas características, también solucionan las vulnerabilidades que se han podido encontrar. Procura utilizar las ultimas versiones de los navegadores (y de todos los programas en general) o mantener éstos al corriente de posibles actualizaciones (parches).
- Defiende tu privacidad: no des tus datos (nombre, e-mail, edad, aficiones, etc) alegremente. Si encuentras un formulario que te pide datos personales, rellena sólo aquellos campos que consideres sean relevantes para el servicio que se ofrece y no des el resto (si son obligatorios, invéntatelos).
- Es buena idea tener una segunda dirección de correo en un servidor gratuito, y usar ésa al rellenar formularios, suscribirte a grupos de noticias, para ponerla en páginas web, etc. Si esta dirección empieza a recibir spam (correo basura, generalmente publicidad no solicitada) puedes olvidarte de ella sin tener que avisar a todo el mundo de que cambias de dirección.
- Cuando envíes copias de un correo a varias personas, pon la lista de direcciones a enviar en el apartado de Bcc o Cco (Blind Carbon Copy o Copia Carbón Oculta) en lugar de utilizar el campo Cc (Carbon Copy), salvo que tengas interés en que se sepa a quien le has enviado copia del correo. De esa forma evitarás que los destinatarios tengan tu lista de correo y puedan hacer un uso indebido de la misma.
- Recuerda que al visitar un servidor web, éste puede saber desde donde te conectas (tu dirección IP). Si lo deseas, puedes navegar anónimamente usando un *anonymizer*, como el de nuestros compas italianos:
  `https://proxy1.autistici.org`
- Recuerda que la comunicación entre tu computadora y otro servidor podría ser interceptada por los puntos intermedios. Para la información importante o confidencial (contraseñas, número de tarjeta de crédito) la comunicación debe ir cifrada con SSL (en la barra del navegador pondrá https en vez de http).
- Usa criptografía (GnuPG o PGP):
  Si no quieres que cualquiera lea tus correos, cifra los correos que mandes, y pide a los demás que cifren los mensajes que te envíen. Así estaréis seguros de que nadie

más lee los mensajes.
Si no quieres que nadie suplante tu identidad (spoofing) o modifique tus mensajes, fírmalos. Para estar seguro de que los mensajes vienen de quien dicen venir, y de que nadie los ha alterado, pide que te los envíen firmados.

- Recuerda que en Internet muchos no son quien dicen ser.
- Utiliza tu sentido común y sé crítico con los contenidos que encuentres.
- Mantente informado en las cuestiones de seguridad. La manera más sencilla es suscribirse al boletín semanal de Kriptópolis: `http://www.kriptopolis.com`
- Si tu computadora está permanentemente conectada a Internet (o aunque sólo lo esté esporádicamente) es buena idea instalar un cortafuegos (firewall) para asegurarse de que no hay accesos desde el exterior. Un módem ADSL en modo multipuesto puede cumplir esta función.
- Si no usas un cortafuegos y utilizas Windows, los intrusos o hackers pueden conseguir acceso cuando está configurado para compartir archivos e impresoras.
  Para deshabilitar compartir ficheros e impresoras en Windows 9x, selecciona: Inicio ⇒ Configuración ⇒ Panel de control, haz doble clic en el icono de Red y seleccione la pestaña de "Configuración". Presiona el botón "Compartir archivos e impresora" y asegúrate de que ambas casillas en el cuadro de diálogo están sin habilitar, "Permitir que otros usuarios tengan acceso a mis archivos" y "Permitir que otros usuarios impriman en mis impresoras".

5. Contraseñas: instrucciones de uso y disfrute

Usa contraseñas fuertes. Hay programas que prueban miles de palabras o secuencias de letras y números, una detrás de otra, buscando la combinación que coincida con tu contraseña. Por seguridad, tu contraseña:

1. No debe ser una palabra de diccionario ni nombre propio, sino que debe contener tanto mayúsculas y minúsculas como números y caracteres especiales (comas, guiones, etc).
2. Debe constar al menos de 5 caracteres (y, según para qué, no más de 8).
3. Debe ser fácil de recordar, ya que anotar la contraseña en algún sitio es la manera más fácil de que alguien la descubra.

Un truco clásico es reemplazar las letras de una palabra por números o símbolos que se les parezcan (Ar@g0n3$ = Aragonés), pero los programas para romper contraseñas ya prueban también esta posibilidad con todas las palabras de su lista.

Un buen truco es utilizar la primera letra de cada palabra de una frase (BNyl7e = BlancaNieves y los 7 enanitos).

En GNU/Linux hay una utilidad llamada pwgen, que genera combinaciones semialeatorias de caracteres que se pueden usar como contraseña.

Algunos consejos:

- Cambia de contraseña de manera regular. Esto no significa que tengas que cambiarla cada día, simplemente que no uses la misma contraseña durante toda la vida. Ante la menor sospecha de que alguien ha podido averiguarla, cambia tu contraseña inmediatamente.
- Nunca la escribas en ningún sitio, y nunca se la reveles a nadie. Si por alguna razón en un momento dado necesitas decirle la contraseña a alguien, vuélvela a cambiar cuanto antes.
- No utilices la posibilidad "Recordar contraseña" que tienen algunos programas.
- No utilices la misma contraseña para todo.