Escrito por Ángel Morán
Jueves, 24 de Octubre de 2002 18:44

Este artículo es una pequeña introducción que contiene una serie de consejos y normas básicas para navegar por internet con una relativa seguridad.

Normas básicas para trastear por Internet y no llevarte un disgusto

Habitualmente no le prestamos demasiada atención a las noticias que circulan acerca de ataques a sitios de internet, hackers... si acaso puede que levantemos un poco la cabeza de detrás del monitor cuando alguien comenta alguna noticia acerca de algún virus de nueva generación, porque, ¿quién no ha tenido alguna vez un virus en su ordenador? Sin embargo el resto de noticias solemos ignorarlas. Al fin y al cabo somos unos pobres e insignificantes usuarios que nada tienen que ofrecer a un atacante exterior.

Sin embargo nos equivocamos; aunque nuestro tiempo de conexión sea breve y nuestras actividades dentro de la red poco interesantes en apariencia, algún día podríamos llevarnos una desagradable sorpresa. Hay muchas maneras de amargarnos la existencia, pero ahora mismo me quedo con dos particularmente molestas:

-

Encontrarte con que has perdido los datos que guardabas en tu equipo por acción de un virus, troyano, gusano o algún bug o fallo de las aplicaciones que utilizas. No solo tus ficheros personales pueden resultar dañados, lo más probable es que los ficheros del sistema hayan resultado dañados, con lo que tu ordenador no funcionará correctamente o incluso podría no arrancar.

-

Descubrir que alguien que no conoces ha utilizado tus datos personales para realizar acciones que nunca serías capaz de cometer: acceso a sitios porno, intentos de intrusión en servidores... tu reputación -y tu ficha policial- puede quedar por los suelos.

Desafortunadamente no hay ningún conjuro ni software infalible que nos sirva para evitar estas situaciones. Sin embargo, una serie de medidas básicas y muy fáciles de seguir pueden minimizar en parte este riesgo. He aquí una lista de ellas:

1.

Intenta hacerte con la última versión del software que utilices. La mayoría de los programas tienen fallos y agujeros de seguridad que aprovecha la gente como puerta de entrada de virus o tomar el control de tu sistema. Las últimas versiones suelen corregir los fallos detectados.

2.

Utiliza un antivirus, pero no una versión de evaluación de esas que vienen en las revistas o te puedes bajar desde internet. Cuando compras un antivirus lo que estás pagando no es el programa en si -que difiere poco o nada de las demos- sino el servicio de actualización de las vacunas y la asistencia técnica. Cada mes suele crearse una media de 10 virus nuevos, con lo que un antivirus sin actualizaciones periódicas es un programa poco eficiente.

Si no quieres pagar licencias, hay antivirus bastante curiosos, como el Inoculate, que son gratuitos. Puede ser una buena opción si no quieres pasar por caja.

3.

No te fies de las apariencias. Los ficheros vbs y js pueden cometer bastantes desaguisados en tu equipo. Los últimos virus que circulan por ahí están hechos en lenguaje vbs (Visual Basic Script) y pueden camuflarse muy fácilmente; si un archivo llamado prueba.vbs lo renombras como prueba.txt.vbs y lo envías adjunto a un mensaje de correo, si el usuario que lo recibe puede creer que es un fichero de texto -libre de sospecha- cuando en realidad es un programa ejecutable. En el caso de Outlook puede ser peor porque en algunos casos puede ejecutar código automáticamente. En ese caso la única solución eficaz sería desactivar el componente de automatización de Visual Basic, que suele venir en las últimas versiones de Internet Explorer o instalado por defecto en Windows 98 y 2000.

No reveles datos personales innecesariamente. Hay muchos sitios donde hay que rellenar un formulario con tus datos antes de pasar de página. En algunos casos sirven para crear un acceso personalizado para el usuario, en otros sólo como estadística y en otros muchos aprovechan estos datos para enviar publicidad a tu cuenta teniendo en cuenta las aficiones que has registrado en el formulario.

Otra cosa: en muchos de estos formularios aparece una casilla marcada por defecto que te pregunta si quieres recibir correo desde el sitio donde te encuentres. A veces puede ser interesante dejarla marcada, pero la mayoría de las veces no.

4.

Utiliza varias cuentas de correo. Hoy día hay un montón de proveedores que facilitan cuentas gratuitas, así que puedes tener una sólo para el correo personal y otra para rellenar los formularios del punto anterior y que si se da el caso de encontrarse saturada de correo basura, no tengas reparo alguno en abandonar.

5.

Los programas de cifrado (PGP y otros) no son tan difíciles de instalar y manejar como pueda parecer. Si utilizas el correo para enviar información confidencial puede ser un punto a tener en cuenta.

6.

Intenta tener el menor número de cookies grabado en tu navegador. No ralentizan el programa ni son fuente de virus, pero a veces pueden decir demasiadas cosas de nosotros y la gente es muy curiosa. Mantén tan solo las indispensables.

7.

Si notas que a tu correo le pasan cosas extrañas, no te cortes. Tú puede que no tengas ni idea de lo que pasa, pero tu proveedor de correo sí -o por lo menos espero que sí. Lo mismo se aplica cuando recibas demasiado correo basura; si no te quejas a quien lo esté mandando, éste entenderá que no te importa recibirlo y seguirá inundándote con mensajes.

Todas estas medidas -y alguna más- son casi elementales y se aplican a cualquier equipo que se conecte, aunque sea por unos minutos- a Internet. Ahora bien, si eres el administrador de una pequeña red que tiene salida a la red o tu acceso te permite estar conectado durante largos períodos de tiempo (por ejemplo con una conexión ADSL) deberíamos tomar unas medidas un poco más serias, pero eso ya lo escribiré en otro rato.