MENORES Y TIC

SEGURIDAD EN INTERNET

ANTONIO GÓMEZ GARCÍA

Mª DOLORES NOGUERAS ATANCE

Índice de contenido

1 INTRODUCCIÓN

A la mayoría de los adultos le resultará familiar la siguiente escena: después de múltiples súplicas, denegaciones y negociaciones al más alto nivel, por fin entra en el hogar el último adelanto tecnológico (léase descodificador TDT, lector/grabador de DVD, reproductor DIVX, cámara o videocámara digital, o por supuesto, EL ORDENADOR). Estamos cerrando el trato con el vendedor o el instalador a domicilio que ya ha dejado el aparatito dispuesto para empezar a funcionar, y antes de despedirse, debe explicar a algún miembro de la familia las funciones más elementales del electrodoméstico en función. ¿A quién acaba exponiéndoselo la mayor parte de las veces?

Correcto. A nuestros hijos. Y a nosotros nos viene bien. " A ellos se les da mejor", pensamos. Y suele ser cierto.

No hace tantos años, nosotros que ahora somos adultos, estábamos al otro lado de la frontera. Cuando entraron los primeros vídeos VHS en nuestras casas, era normal que papá (o más normalmente mamá) se encargaran del uso del mando a distancia, porque "era un aparato muy caro para dejarlo en manos de los niños", durante no más de dos semanas, hasta que se rendían a la realidad de que nosotros sabíamos manejarlo mucho mejor y no teníamos problemas para reproducir una película, grabar un programa en el canal adecuado e incluso programar el vídeo para que grabara un programa de manera autónoma a horas intempestivas. El vídeo acababa siendo parte de nuestros dominios dentro de casa.

El caso es que ahora la cosa ha cambiado. Y mucho. La cosa no está en programar un vídeo, o sintonizar los canales de la nueva "tele". Ahora estamos hablando de videoconsolas, teléfonos móviles con capacidad de grabación de vídeo y envío de mensajes SMS, tarjetas de memoria, cámaras digitales, y nuestra pesadilla: EL ORDENADOR. INTERNET.

Internet es una ventana abierta al mundo. Cuando un niño se conecta a Internet, es como si saliera al mundo exterior. Y cuando un hijo nuestro sale a la calle, podemos otorgarle un cierto grado de autonomía (no podemos acompañarle continuamente), pero sí nos gusta saber con quién va, qué sitios visita y qué tipo de actividades suele realizar.

Por eso no podemos imitar a nuestros propios padres en esto. Es cierto que hay un salto generacional muy grande, y que nuestros niños tienen una capacidad de trabajo con las nuevas tecnologías de las que nosotros está claro que carecemos o, por lo menos, no tenemos al mismo nivel. Pero no podemos IGNORAR lo que hacen. ELLOS TIENEN LA CAPACIDAD, PERO NOSOTROS TENEMOS LA EXPERIENCIA.

Ellos saben cómo funcionan las nuevas tecnologías. Pero nosotros sabemos (al menos, en parte), como funciona el mundo. Está claro que deberemos avanzar juntos.

2 ¿QUÉ PODEMOS HACER PARA PROTEGER A NUESTROS HIJOS?

De momento, INTERESARNOS POR LO QUE HACEN. No podemos "aprender informática en una tarde", y mucho menos ponernos a su nivel. Tampoco es el objetivo de esta exposición. Y tampoco debemos creer que nuestros hijos sean unos expertos en estas tecnologías, salvo en aquella parte que usan normalmente, porque la han incorporado a sus vidas: chat, e-mail, sms...

Podemos empezar por aquí. El cuerpo principal de esta charla va a tener cuatro partes bien diferenciadas, pero complementarias entre sí:

- MARCO LEGAL: ¿qué grado de responsabilidad civil y penal puede tener un menor cuando navega por Internet?. ¿Y un adulto?. ¿Qué es delito y qué no?. ¿Qué es eso del "pirateo"?
- ACTIVIDADES COMUNES DE LOS ADOLESCENTES EN INTERNET: aprenderemos, independientemente de nuestros conocimientos informáticos, en qué consisten palabras comunes en su vocabulario como chat, foros, Youtube, virus, troyanos, firewall, crack, hacker...
- PELIGROS DERIVADOS DE DICHAS ACTIVIDADES: si sabemos qué tipo de actividades llevan a cabo nuestros hijos en el ciberespacio, y qué consecuencias puede tener una mala actuación o comportamiento descuidado, o la pura y simple mala suerte, podemos estar más preparados para ayudarles y protegerles.
- NORMAS BÁSICAS DE SEGURIDAD: no hace falta ser un experto informático para garantizar, al menos, unas pautas de seguridad básicas en nuestra casa de cara a Internet.

3 MARCO LEGAL.

3.1. Responsabilidad civil y penal

Como es obvio para cualquiera que me conozca, no soy abogado, y reconozco que mis conocimientos en materia legal son, por calificarlos de manera generosa, poco menos que limitados. Sin embargo, sí sé algunas cosas que pueden resultarle útiles:

A) LOS DELITOS Y FALTAS COMETIDOS A TRAVÉS DE O UTILIZANDO INTERNET SON DIFÍCILES DE DEMOSTRAR: Internet es una red MUNDIAL de ordenadores. En el momento en que se comete un delito o falta en un país desde un ordenador radicado en otro distinto, se producirá un conflicto entre los códigos civiles o penales de ambos países. Lo que es delito en uno, puede no serlo en otro. La policía de un país no puede investigar libremente al súbdito de otro país sin colaboración de sus propias fuerzas de seguridad, de modo que normalmente sólo se investiga si el delito es lo suficientemente probado y perjudicial como para que INTERPOL tome cartas en el asunto (delitos de corte sexual o fraudes económicos cuantiosos).

Por otro lado, se puede rastrear el ordenador desde el que se ha cometido el delito, pero después hay que probar quién era el que lo estaba operando. Empiezan a surgir casos en los que un "hacker" o pirata informático infecta mediante un troyano el ordenador de otra persona, con el objetivo de controlarlo y realizar sus actividades delictivas desde ese segundo ordenador, de modo que es su inocente propietario quien puede encontrarse después con las consecuencias.

B)EL GRADO DE RESPONSABILIDAD CIVIL DE UN ADULTO EN ESPAÑA, ES, SEGÚN ESO, MUY BAJO: puede requerírsele legalmente en determinadas situaciones, pero debe probarse la acusación bajo circunstancias ciertamente muy restrictivas.

C)EN CONSECUENCIA, EL GRADO DE RESPONSABILIDAD PENAL ES TAMBIÉN MUY BAJO.

D) ERGO, EL GRADO DE RESPONSABILIDAD CIVIL Y PENAL DE UN MENOR DE EDAD EN ESPAÑA en actividades delictivas relacionadas con las nuevas tecnologías, según la legislación actual, ES PRÁCTICAMENTE NULA.

3.2. ¿Qué es delito en Internet?

- La obtención ilícita y el tráfico de datos personales
- Las estafas económicas superiores a los 300 €
- Distribución de material pornográfico en el supuesto de que se distribuya entre menores o

sea protagonizado por menores

- Los delitos contra la propiedad intelectual si existe ánimo demostrado de lucro (el hecho de "bajarse" películas o canciones de Internet no es considerado delito, salvo si existe un intercambio económico; la venta de películas piratas, el famoso "top manta", sí está catalogado como tal)

3.3. ¿En qué situación puede mi hijo estar cometiendo un delito relacionado con las nuevas tecnologías?

- Cuando distribuye copias de material con propietario intelectual (películas, canciones...) a cambio de dinero
- Cuando obtiene y distribuye información o imágenes de carácter sexual, humillante o degradante de otra persona sin su consentimiento expreso
- Cuando utiliza las nuevas tecnologías para acosar, humillar, calumniar... a otra persona.

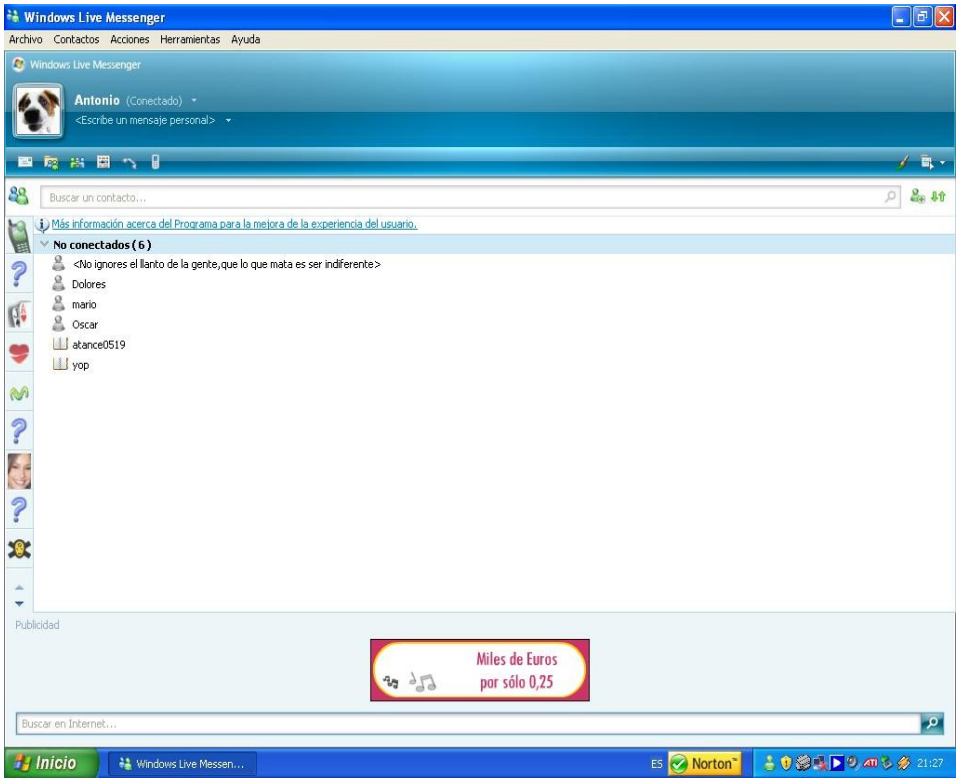
3.4. ¿Cuándo puedo denunciar un delito contra mi hijo?

- Cuando está siendo acosado por sus compañeros
- Cuando se está obteniendo y utilizando fraudulentamente información relacionada con su persona
- Cuando está siendo objeto de acoso sexual

4 HERRAMIENTAS INFORMÁTICAS MÁS COMUNES ENTRE ADOLESCENTES.

A) MENSAJERÍA INSTANTÁNEA.

Es el famoso “Messenger”. Se trata de un programa residente en memoria en el ordenador, que tiene una lista de las direcciones de correo “agregadas” por el usuario como amigos, y que le avisa cuando se conecta alguno de ellos, permitiéndole llevar a cabo una conversación en tiempo real, por escrito, o si se tiene cámara web, en directo, por videoconferencia.

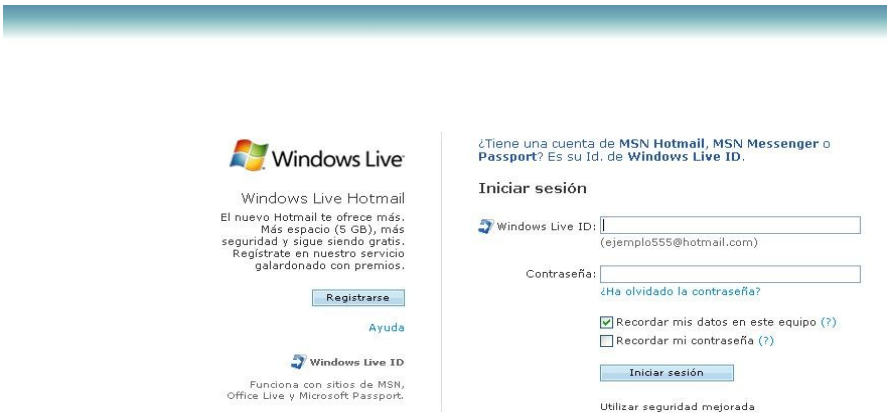


No debería haber mucho problema mientras la dirección de correo del niño sea conocida sólo por sus amigos. El problema viene cuando esta dirección puede ser aprehendida por alguien poco escrupuloso.

B) CORREO ELECTRÓNICO

Un servicio de correo electrónico permite al usuario enviar y recibir mensajes de texto con imágenes y, en ocasiones, archivos adjuntos que puede descargar en su ordenador. Un archivo adjunto es algo así como un "paquete" certificado que puede contener información de todo tipo. Este es el camino que escogen algunos virus y troyanos para infectar nuestro ordenador.

Para poder utilizar un servicio de correo electrónico, el usuario debe contar con una dirección y una contraseña de acceso.

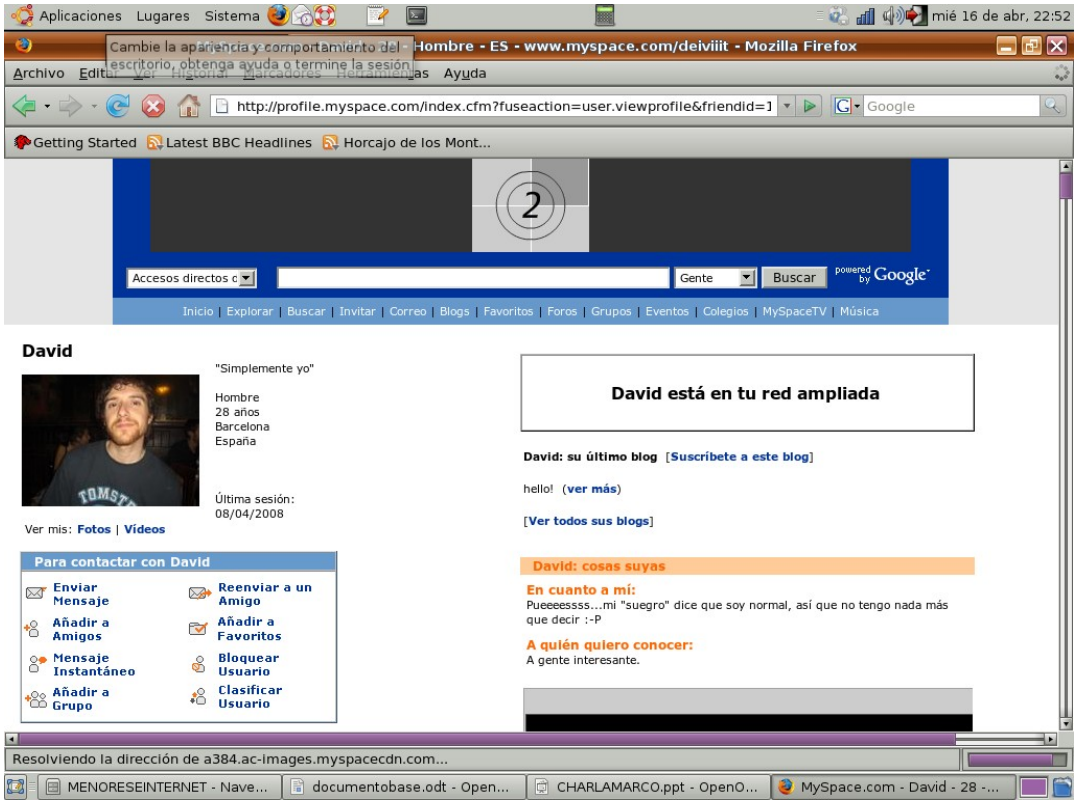


Cuando se accede a un ordenador compartido (por ejemplo, un cibercafé, la escuela o instituto, etc...) es importante procurar no dejar marcadas las opciones que suelen ofrecer estos servicios de recordar la dirección y contraseña utilizados, para que un usuario posterior no tenga acceso a los mensajes que nos envían.

C) ESPACIOS WEB PREDISEÑADOS

Hoy en día, para crear una página web accesible desde cualquier punto del planeta, no es necesario tener un conjunto específico de conocimientos técnicos. Basta con acceder a determinados portales donde se nos ofrece, previo registro, la posibilidad de alojar contenidos con textos e imágenes propias, completamente configurables y reordenables a voluntad. Entre estos tipos de espacios web, brillan con luz propia los blogs y fotologs.

UN BLOG ES UN ESPACIO EN EL QUE EL USUARIO PUEDE GRABAR TEXTOS E IMÁGENES ACCESIBLES PARA OTROS USUARIOS, ORGANIZADOS NORMALMENTE POR ORDEN CRONOLÓGICO.



UN FOTOLOG ES UN ESPACIO SIMILAR A UN LOG, PERO EN EL QUE LA MAYORÍA DE CONTENIDOS SE BASAN EN FOTOGRAFÍAS PERSONALES. LAS ACTUALES REDES SOCIALES SON EL SIGUIENTE PASO EN LA ESCALA EVOLUTIVA DE LOS FOTOLOGS.

Entre todos estos espacios, MYSPACE es el más popular entre los adolescentes, que además permite crear enlaces que llevan a las páginas de otros amigos del usuario sólo con pinchar con el ratón encima de ellos.

D) FOROS DE INTERCAMBIO

Un foro es un espacio en el que un usuario propone un tema, escribiendo sobre él. El resto de los usuarios pueden leer el tema, y contestar si les apetece. Es como tener una pizarra en la que cada persona que va llegando va dejando escrito aquello que más le apetece.

E) CANALES IRC. SERVICIOS DE CHAT

Los servicios de chat, o canales IRC, son servicios en los que el usuario, al conectarse, comparte una página en la que se comunica con otros usuarios en tiempo real, al estilo de la mensajería instantánea, pero sin conocer a los otros internautas.

En estos servicios, todos los usuarios pueden hablar con todos en público o en privado. Se dice que un usuario "susurra" a otro o le solicita un "privado" cuando se comunica con él sin que los demás se enteren de lo que se está diciendo.

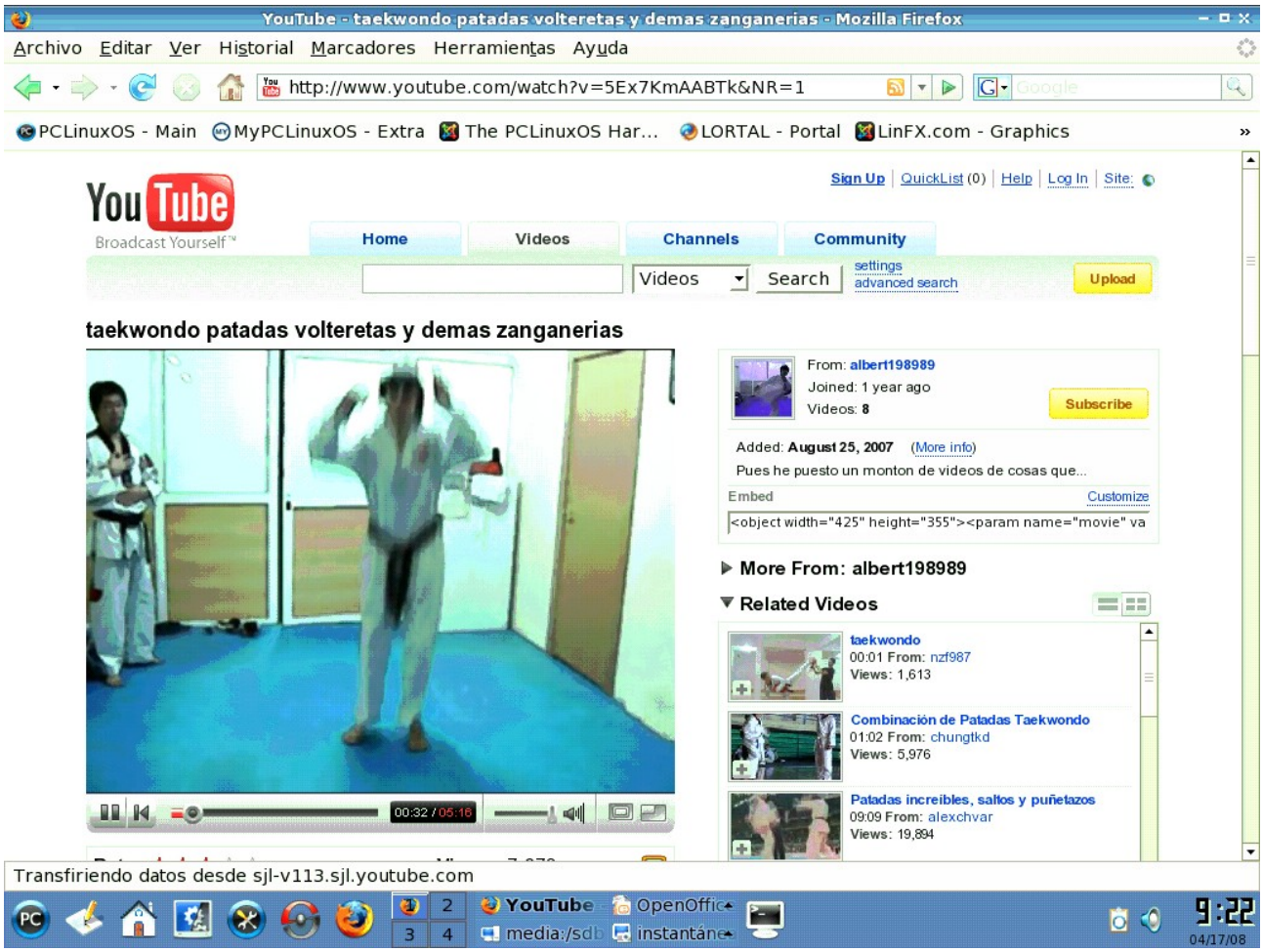
Las salas o canales de chat suelen contar con uno o varios administradores que cuentan con la posibilidad de permitir o denegar el acceso a los distintos servicios del chat a los usuarios. Si un internauta es maleducado o incumple con las normas, puede expulsársele del servicio (se le "banea").

F) VIDEOESPACIOS. YOUTUBE.

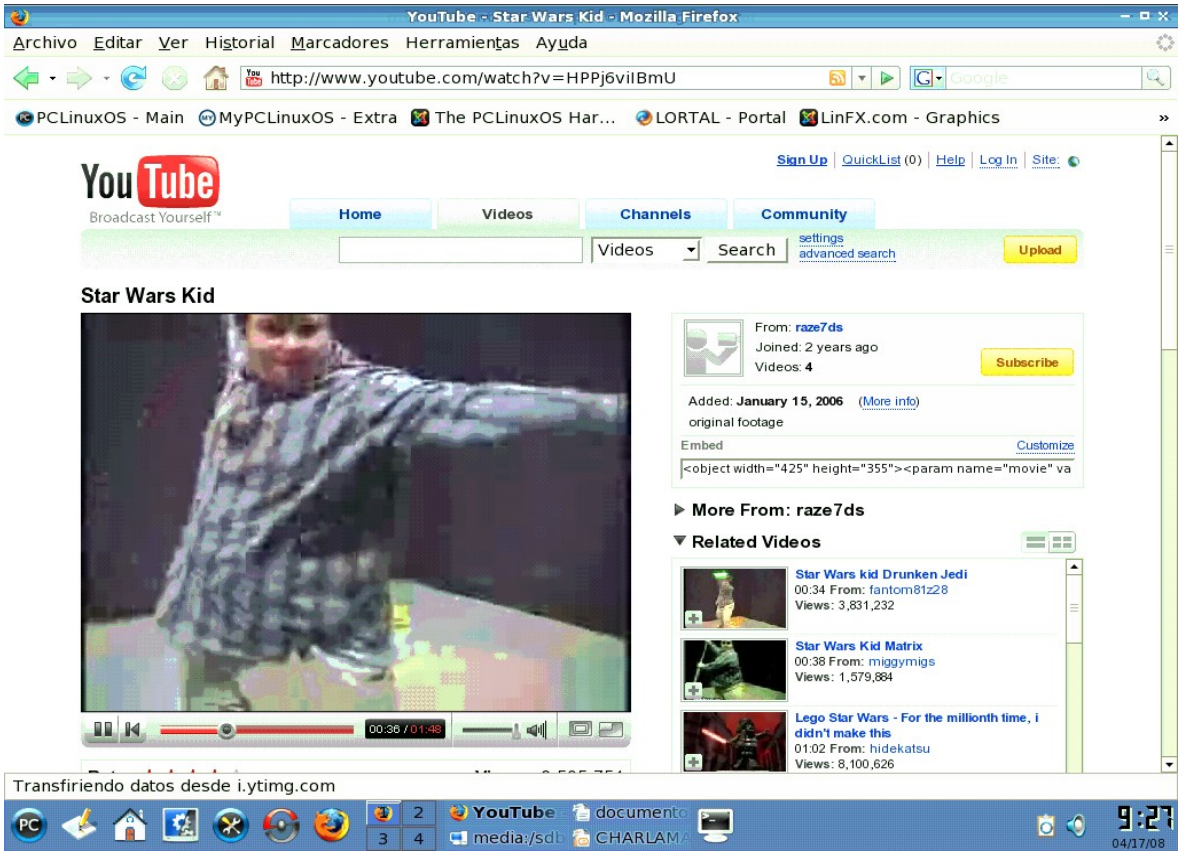
Podemos entender por videoespacios aquellas páginas o portales en Internet en la que cualquier usuario puede dejar grabado un vídeo propio muy fácilmente, sin más requisitos que el haberse registrado previamente. La estrella de este tipo de espacios es el famoso Youtube:

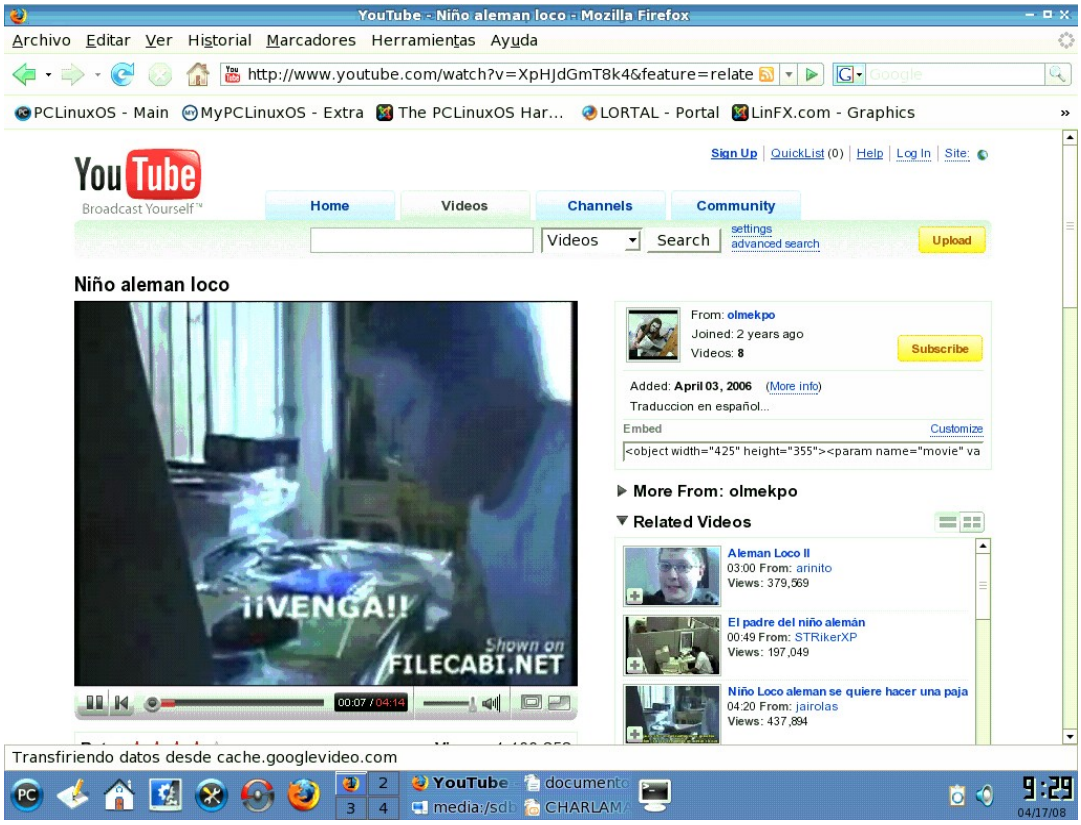
Estos espacios digitales se apoyan en el uso de tecnologías Flash, que permite empezar a ver el vídeo antes incluso de que se haya descargado del todo, lo que unido a la creciente velocidad de las lineas de conexión a Internet ha popularizado el uso de este tipo de comunidades online. No hace falta decir que su mención casi rutinaria en el espacio de varios telediarios y programas televisivos de zapping ha potenciado más aún su utilización por parte de los adolescentes, que quieren tener

(como todos) sus quince minutos de fama.



El mayor peligro de estas herramientas de comunicación está en la rapidez con que se pueden expandir determinadas acciones de tipo humillante o vejatorio, como es el tristemente famoso caso del “Star Wars Kid” o “el niño alemán enfadado”

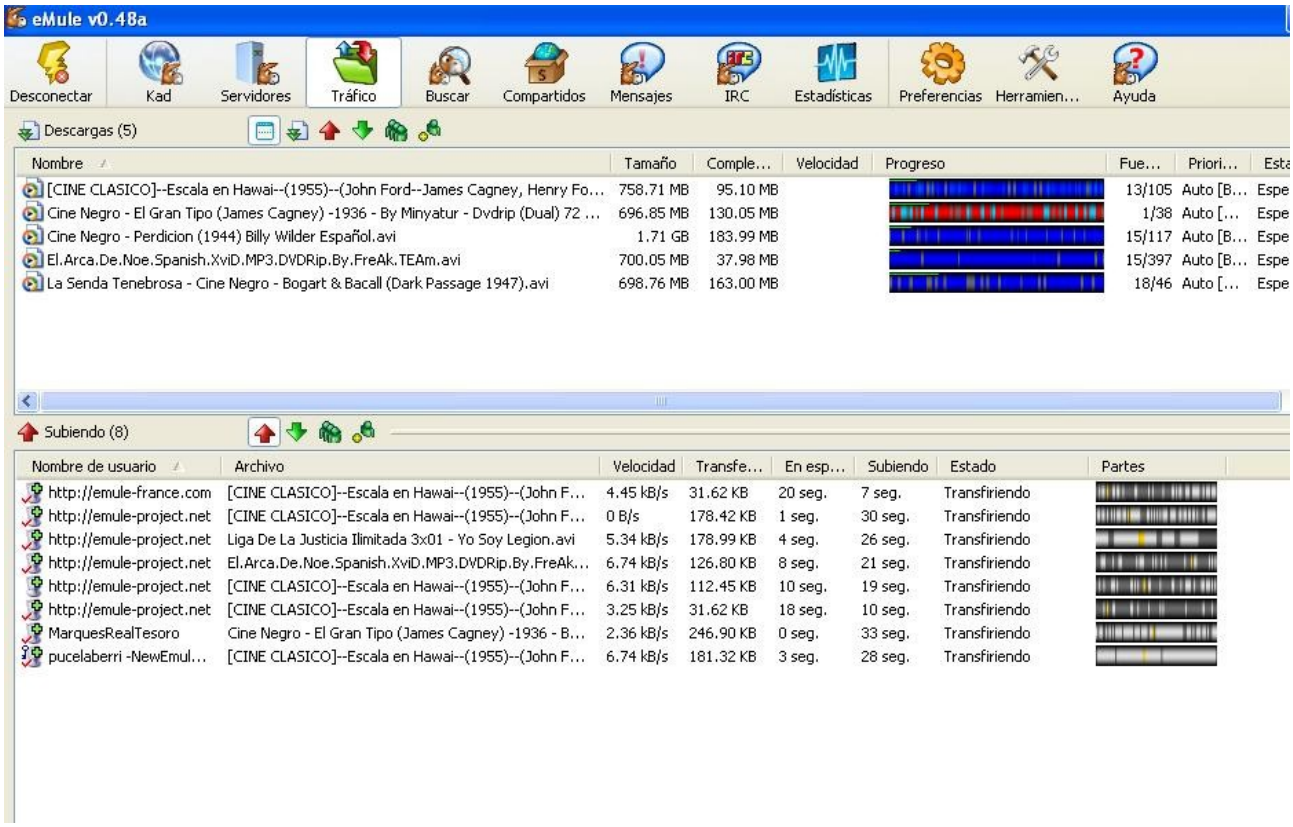

YouTube - Star Wars Kid - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://www.youtube.com/watch?v=HPPj6viIBmU
PCLinuxOS - Main
MyPCLinuxOS - Extra
The PCLinuxOS Har...
LORTAL - Portal
LinFX.com - Graphics
Sign Up | QuickList (0) | Help | Log In | Site:
YouTube
Broadcast Yourself
Home
Videos
Channels
Community
Videos
Search
settings
advanced search
Upload
Star Wars Kid
From: raze7ds
Joined: 2 years ago
Videos: 4
Subscribe
Added: January 15, 2006 (More info)
original footage
Embed
Customize
<object width="425" height="355"><param name="movie" va
More From: raze7ds
Related Videos
Star Wars kid Drunken Jedi
00:34 From: fantom81z28
Views: 3,831,232
Star Wars Kid Matrix
00:38 From: miggymigs
Views: 1,579,884
Lego Star Wars - For the millionth time, i didn't make this
01:02 From: hidekatsu
Views: 8,100,626
00:36 / 01:48
Transfiriendo datos desde i.ytimg.com
YouTube
documento
media:/sdb
CHARLAMA
9:27
04/17/08


YouTube - Niño aleman loco - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://www.youtube.com/watch?v=XpHJdGmT8k4&feature=relate
PCLinuxOS - Main
MyPCLinuxOS - Extra
The PCLinuxOS Har...
LORTAL - Portal
LinFX.com - Graphics
Sign Up | QuickList (0) | Help | Log In | Site:
YouTube
Broadcast Yourself
Home
Videos
Channels
Community
Videos
Search
settings
advanced search
Upload
Niño aleman loco
¡¡VENGA!!
Shown on
FILECABI.NET
From: olmekpo
Joined: 2 years ago
Videos: 8
Subscribe
Added: April 03, 2006 (More info)
Traduccion en español...
Embed
Customize
<object width="425" height="355"><param name="movie" va
More From: olmekpo
Related Videos
Aleman Loco II
03:00 From: arinito
Views: 379,569
El padre del niño alemán
00:49 From: STRikerXP
Views: 197,049
Niño Loco aleman se quiere hacer una paja
04:20 From: jairolas
Views: 437,894
00:07 / 04:14
Transfiriendo datos desde cache.googlevideo.com
YouTube
documento
media:/sdb
CHARLAMA
9:29
04/17/08

G)PROGRAMAS P2P DE INTERCAMBIO DE ARCHIVOS

Los programas P2P (Peer to Peer), entre los que reinan E-mule, Ares y Bit Torrent, son programas que permiten a los usuarios intercambiar archivos entre sus respectivos ordenadores. Para ello, tienen que dejar que el programa marque una carpeta de su ordenador como “compartida”, para que el resto de los usuarios puedan bucear en ella y obtener una copia de los archivos que les interesen (canciones, películas, etc...).

Así, cuando un usuario de E-mule busca una película con un título determinado, por ejemplo, “Tarzán”, sólo tiene que introducir el criterio de búsqueda, y a los pocos segundos el programa le pone en contacto con los ordenadores de otros usuarios que contienen archivos con ese nombre.



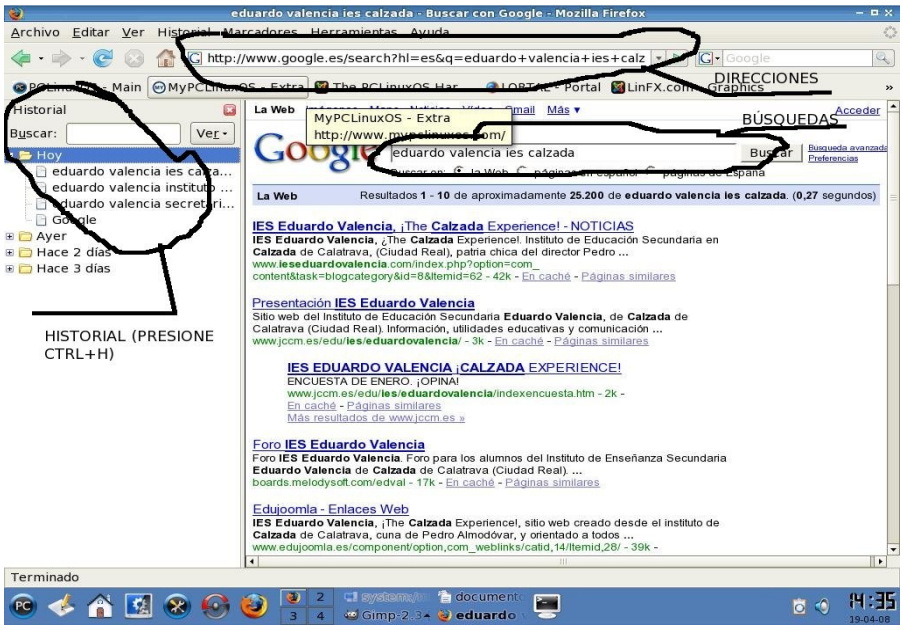
Estos programas traen implementado un sistema de puntuaciones por medio del cual, aquellos usuarios cuyos archivos sean más solicitados, pueden descargar a su vez los archivos que desean a mayor velocidad, llevados por la filosofía de “el que más comparte, tiene más derechos”. Un sistema eficaz que sin embargo, conduce a veces a la picaresca de que algunos usuarios cambian el nombre de sus archivos por otros más atractivos. Es bastante frecuente que un usuario de programas P2P crea estar “bajándose” la última película que aún colea en la cartelera, y luego se encuentre con “sorpresas” como películas pornográficas.

Los programas de intercambio también suelen suponer una excelente vía de propagación para virus y troyanos que infectan programas populares muy descargados por los usuarios P2P.

H) WORLD WIDE WEB. NAVEGACIÓN POR LA RED

Por ser la más conocida, y además ser la base por la que se necesita pasar forzosamente para acceder a todas las otras herramientas, es precisamente por lo que la hemos dejado para el último lugar.

Los usuarios de la WWW utilizan un programa denominado explorador, normalmente el INTERNET EXPLORER o el MOZILLA FIREFOX, que suele arrancar en una página web de inicio llamada MOTOR BUSCADOR (por ejemplo, GOOGLE, YAHOO, o TERRA) en la que se le ofrece introducir directamente la dirección del sitio web que esté buscando, si se conoce (ej: www.ieseduardovalencia.com), o utilizar el formulario de abajo para introducir criterios de búsqueda conforme a los cuales el buscador le ofrecerá varias posibilidades (en el mismo ejemplo, eduardo valencia ies calzada). Una vez se ha entrado en una página, normalmente el usuario se va moviendo por distintos contenidos sólo pinchando con el ratón en textos o imágenes denominados hipervínculos o enlaces.



ES INTERESANTE LA HERRAMIENTA HISTORIAL DE ESTOS EXPLORADORES (POR DEFECTO, SE OBTIENE PULSANDO LAS TECLAS CTRL+H), QUE NOS MUESTRA LAS PÁGINAS VISITADAS POR ORDEN CRONOLÓGICO. AÚN MÁS INTERESANTE RESULTA QUE PRECISAMENTE UNA DE LAS HABILIDADES QUE ANTES APRENDEN LOS ADOLESCENTES ES, PRECISAMENTE, BORRAR DICHO HISTORIAL.

I) LAS REDES SOCIALES

En el momento de escribir estas líneas, son precisamente las redes sociales la principal causa de preocupación para padres y educadores, en el mismo grado en que causan furor entre nuestros jóvenes.

En un principio, una red social viene a ser algo así como la unión de la mayoría de los servicios que hemos comentado en apartados anteriores. Estos servicios permiten al usuario, previo registro, contar con un espacio propio donde pueden escribir lo que quieran, colgar fotos, ponerse en contacto con otros usuarios, vía mail, foros, chat...

Lo más atrayente de estas herramientas es su espontaneidad e inmediatez. El adolescente tiene la sensación de tener una segunda vida en el ciberespacio, donde tiene relación social, no solo con su entorno habitual, sino, y ahí radica el peligro, con otros usuarios de la red con los que poco a poco va tomando contacto, y de los que sólo sabe lo que ellos le cuentan, y a la recíproca.

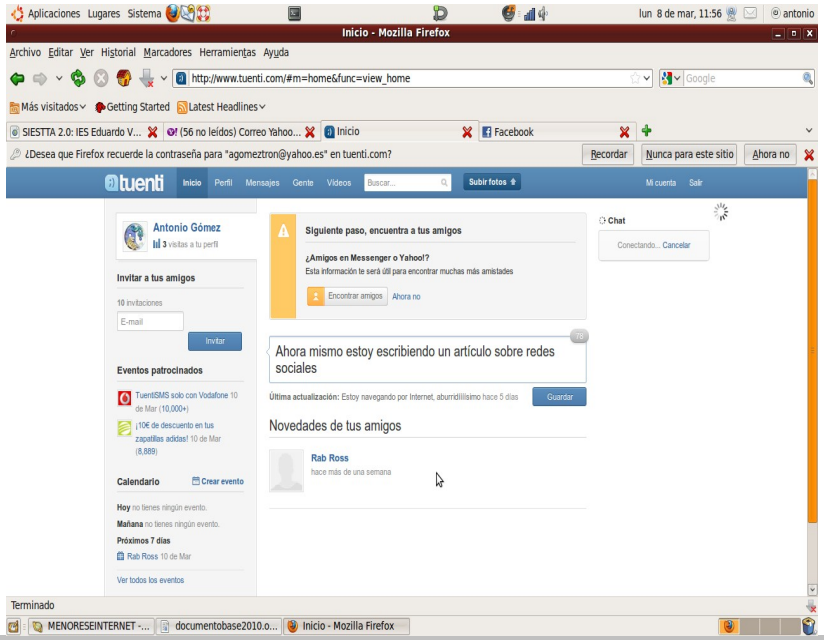
En la actualidad, las redes sociales más utilizadas en nuestro entorno son:

- TUENTI (http://www.tuenti.com)
- FACEBOOK (http://es-es.facebook.com/)
- TWITTER (http://www.twitter.com)
- FOTOLOG (http://www.fotolog.com)
- MYSPACE (http://www.myspace.com)

La estructura de una red social incluye (de forma común) los siguientes elementos:

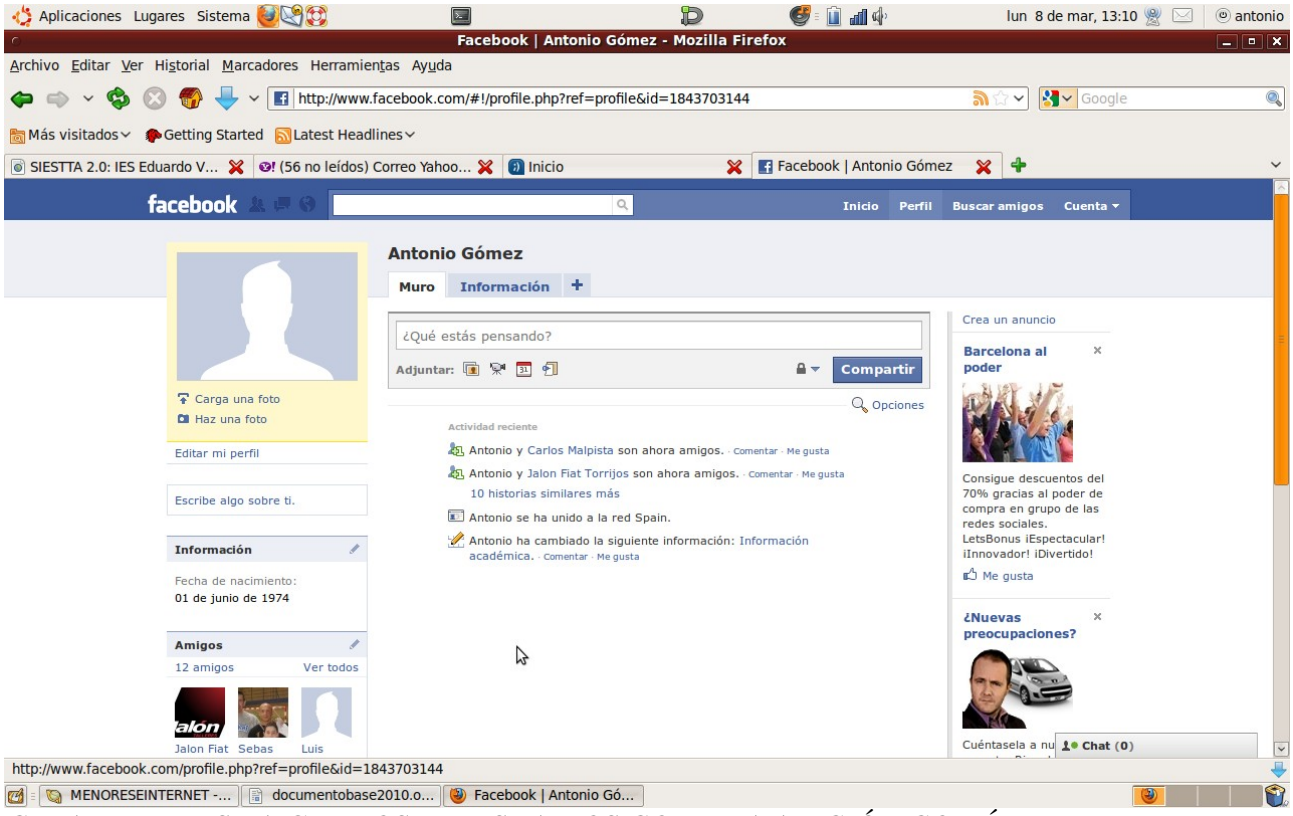
PÁGINA DE INICIO

Al conectarse el usuario, dando nombre y contraseña, la primera página web que aparece en el monitor informa sobre los cambios sucedidos desde la última vez que entró en la red social: los nuevos usuarios que desean contactar con nosotros (“hacerse amigos”), mensajes que nos han enviado, grupos nuevos que se han creado y que podrían interesarnos...



PERFIL PROPIO DE USUARIO

En este perfil, una página web prefabricada, el usuario habla sobre sí mismo, cuelga fotografías, escribe lo que está haciendo en este momento... es, digamos, la cara del usuario que se va a mostrar a otros usuarios. Algunas redes sociales, como Tuenti, incorporan la posibilidad de que el usuario elija qué partes de su perfil sean públicas (cualquier otro internauta puede verlo), o visibles sólo para sus amigos (otros internautas que el usuario ha confirmado que conoce en la red). Esta es la parte en la que el adolescente puede mostrarse más vulnerable, puesto que es donde está introduciendo información de carácter personal.



CREAR Y UNIRSE A GRUPOS DE USUARIOS CON UNA AFICIÓN COMÚN

A medida que se progresa en el uso de estas herramientas, es fácil contactar con otros usuarios con aficiones comunes. En ocasiones, se nos puede proponer (o la iniciativa puede partir de nosotros mismos), crear un grupo determinado, con la intención de que otros internautas se solidaricen con nuestra causa. Puede haber tantos motivos como personas, y aún más; desde POR LA RECONCILIACIÓN Y LA CONCORDIA ENTRE TODOS LOS PAÍSES, hasta grupos que buscan defender POR LOS DERECHOS DE LOS QUE QUIEREN ANDAR CON LAS MANOS Y BEBER CON LOS PIES. El hecho de pertenecer a un grupo posibilita aumentar la cantidad de contactos con otras personas, además de fomentar la solidaridad y la colaboración en causas que pueden resultar atractivas para el niño o adolescente.

CREAR Y MANTENER UN "MURO" DE FOTOS Y FIRMAS, O SISTEMAS DE COMENTARIOS

Esta es una de las aplicaciones más utilizadas por los adolescentes, que les ayuda a mantener un "status" de "prestigio social". Aquél que logre más comentarios de amigos y otros internautas, será el más popular en su entorno virtual, e incluso social. Incluso para nosotros, los adultos, resulta algo realmente adictivo comprobar, cada vez que estamos cerca de un ordenador, si se ha producido algún cambio en nuestro perfil, si alguien nos ha contestado un mensaje, si el grupo que hemos creado está atrayendo a mucha gente, etc...

Hace relativamente poco tiempo, saltó a varios medios de la prensa escrita y online la noticia de un ladrón que fue pillado porque se paró a comprobar su cuenta en Facebook en la vivienda que estaba allanando, y luego no cerró la puerta. La policía sólo tuvo que examinar su perfil, y pocas horas después, presentarse en la casa del ladrón, para pedirle educadamente que les acompañara. No he podido contrastarlo más que por un par de sitios web de noticias, pero el lector convendrá conmigo que la idea, aunque fuera una leyenda urbana, merecía comentarse aquí.

CALENDARIO DE EVENTOS

Esta herramienta, común a la mayoría de las redes sociales, consiste en mantener una especie de calendario en común, donde los usuarios que comparten un grupo dentro de la red social, pueden agregar eventos en las fechas deseadas. Así, por ejemplo, puedo informar (práctica bastante extendida) sobre mi cumpleaños a mis amigos, o a la totalidad de la red, dependiendo de las opciones de configuración.

Esta herramienta tiene tal poder de convocatoria que suele ser ya un clásico en los informativos de TV; es mediante la creación de grupos y posterior convocatoria de eventos que se han organizado desde macrobotellones ilegales en zonas costeras, a manifestaciones a favor o en contra de determinados grupos, personas o ideas políticas.

5 PELIGROS MÁS COMUNES.

Una vez expuestas, de manera bastante esquemática, las principales tecnologías de la comunicación utilizadas hoy en día por nuestros adolescentes, procede realizar una enumeración de los peligros que llevan aparejados.

Como no es nuestra intención elaborar una enciclopedia, y sabiendo siempre que la tecnología avanza muy rápidamente, y no podemos pretender resumir en este documento todos los riesgos que un menor puede encontrarse en su periplo por la web, nos limitaremos a enumerar las prácticas a nuestro juicio más peligrosas: infección por virus o troyanos, el Phising, el Child Grooming, las estafas y fraudes telemáticos y el Ciberbullying.

5.1. Infección por virus y troyanos.

Un virus informático es un programa que se instala en nuestro ordenador sin nuestro conocimiento con propósitos destructivos. . Además, en prevención de que podamos detectarlo e intentar borrarlo, y a semejanza de los virus auténticos, hace diversas copias de sí mismo y las va distribuyendo por distintas zonas del disco duro.

Aunque pueda parecernos imposible, hay mucha gente dispuesta a gastar su tiempo creando códigos maliciosos que puedan perjudicar a nuestros equipos, por motivos tan peregrinos como la satisfacción de superar a programas antivirus creados por informáticos profesionales, o infectar a suficientes equipos en un momento dado como para ser mencionados en los telediarios y otros medios de prensa de que hablábamos antes, para conseguir los dichosos quince minutos de fama.

Un troyano es un programa que también se instala en nuestro ordenador sin nuestro conocimiento ni permiso, pero en esta ocasión su objetivo es pasar completamente desapercibido mientras deja abierta una "puerta trasera" o backdoor que permite al pirata informático controlar su funcionamiento.

Así, un ordenador infectado por un troyano puede reunir toda la información que le resulte interesante al pirata informático, como pueden ser contraseñas, números de cuenta, datos bancarios... y enviárselo sin que nos enteremos. En otras ocasiones, puede ser que el hacker utilice nuestro equipo para cometer un delito, con el objeto de emborronar su pista. Si se rastrea la actividad delictiva con éxito, adonde acudirá el investigador será a nuestro propio domicilio. También han tenido cierto éxito los programas que nos conectan sin nuestro permiso a servicios de pago, cuya cuota nos llegará a final de mes junto a la factura telefónica, si bien esta última práctica empieza a ser atajada.

Los dos canales más utilizados por estos programas para infectar nuestros ordenadores son:

a) El correo electrónico: de por sí, un mensaje de texto no tiene peligro alguno. Podemos leer un correo enviado por un desconocido sin problema alguno. Pero si ese correo tiene un archivo adjunto que se nos propone que abramos, y desconocemos su procedencia, deberíamos borrar el mensaje sin pensarlo.

b) El software de procedencia dudosa (léase los programas “piratas” que nos bajamos o conseguimos en páginas ilegales) puede también perfectamente incluír este tipo de “sorpresitas”

c) La navegación por determinadas páginas web, normalmente también de dudosa catadura ética y moral.

5.2. Phising y otras formas de estafas informáticas

En la línea de aquellos antiguos especialistas en el arte del escamoteo y del timo, permanecen ciertas prácticas que se apoyan no tanto en los superiores conocimientos informáticos del delincuente como en la ingenuidad o en la necesidad del estafado de creer que por una vez en la vida va a tener suerte, o incluso, en los casos más ingeniosos, aprovecharse de la avaricia de la víctima.

¿De qué estamos hablando exactamente?. Vayamos por partes:

Se ha dado en llamar phising a la práctica en la que el delincuente envía un mensaje haciéndose pasar por una entidad bancaria en la que explica que el banco ha tenido determinadas dificultades técnicas y necesita que el cliente vuelva a introducir sus datos bancarios para comprobar su base de datos, o una excusa por el estilo.

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

No es necesario decir que nuestro banco nunca nos pedirá ningún tipo de datos personales, y que este tipo de gente no planea nada nuevo para nuestra economía familiar.

Si bien este tipo de amenazas no están orientadas a nuestros hijos tanto como a nosotros, nos ha parecido bien comentarlas como introducción a una forma de actividad fraudulenta que es más posible que se orienten hacia ellos; hablemos, pues, del concepto de INGENIERÍA SOCIAL.

En Internet, se entiende como INGENIERÍA SOCIAL el conjunto de prácticas que tienen como objetivo obtener beneficios de una persona aprovechando su ingenuidad e inocencia, y por qué no decirlo, su creencia firme en que puede tener suerte, ser el elegido, al menos por una vez en la vida.

Así, es común recibir correos electrónicos en los que se nos ofrece, por ejemplo, abrir una cuenta en un pequeño y extraño paraíso fiscal, a donde se nos irán destinando, sin ningún esfuerzo por nuestra parte, los fondos ingresados por mafiosos, guerrilleros o políticos corruptos que no podrán hacer nada por evitarlo dado que no pueden denunciarnos sin autoinculparse.

También es común encontrarnos, navegando por Internet, con pequeños mensajes emergentes en los que se nos felicita porque somos el visitante nº X, y nos corresponde un maravilloso premio que se

nos entregará si pinchamos AQUÍ, o llamamos al número XXXXXXXX. ¿Les suena de algo la historia?.

5.3. El "Child Grooming"

Llegamos a una de las prácticas delictivas que, por su presencia diaria en los medios de comunicación, más han llegado a preocuparnos como padres.

La práctica denominada GROOMING consiste en el acoso, chantaje, coacción... a un menor utilizando las nuevas técnicas de la información y de la comunicación.

El anonimato y la facilidad de acceso a todo tipo de información que ofrece Internet facilita a cualquier persona carente de escrúpulos la oportunidad de contactar con un menor de edad haciéndose pasar por otra persona completamente distinta, normalmente otro menor, y aprovechar su mayor madurez para tomar una posición de superioridad sobre el niño que le permita obligarle a realizar acciones que por sí solo no haría.

Quizás sea más explícito este ejemplo, extracto tomado de un artículo de *EL* PAÍS; esta conversación, que el periodista aclara es perfectamente ficticia, se supone que tiene lugar en una sala de chat:

Carlos_25. Hola eres mujer?

Lucia13. Chica y tu?

Carlos_25. Hombre q edad tiens?

Lucia13. Pues la q ves, 13 Y tu? eres un poco mayor.

Carlos_25. Tengo 17.

Lucia13. D dnd eres?

Carlos_25. Venezuela tu?

Lucia13. Madrid España no tienes 25?

Carlos_25. No tienes msn?

Lucia13. No se lo voy a dar a un desconocido.

Carlos_25. Te gusta hablar de sexo?

Lucia13. No se de sexo.

Carlos_25. Yo te enseño.

Lucia13. El q?

Carlos_25. El sexo.

Lucia13. No se me da miedo.

Carlos_25. Es algo normal.

Lucia13. Xq no quieres hablar de otra cosa?

Carlos_25. Es q estoy solo quiero calentarme.

Lucia13. No quiero seguir hablando.

Carlos_25. A ti ya te salieron pelitos en tu vagina?

Lucia13. Adios.

Si bien el artículo aclara que es un diálogo imaginario, refleja a la perfección una posibilidad real de peligro para nuestros hijos en la que preferimos no pensar por que nos aterroriza.

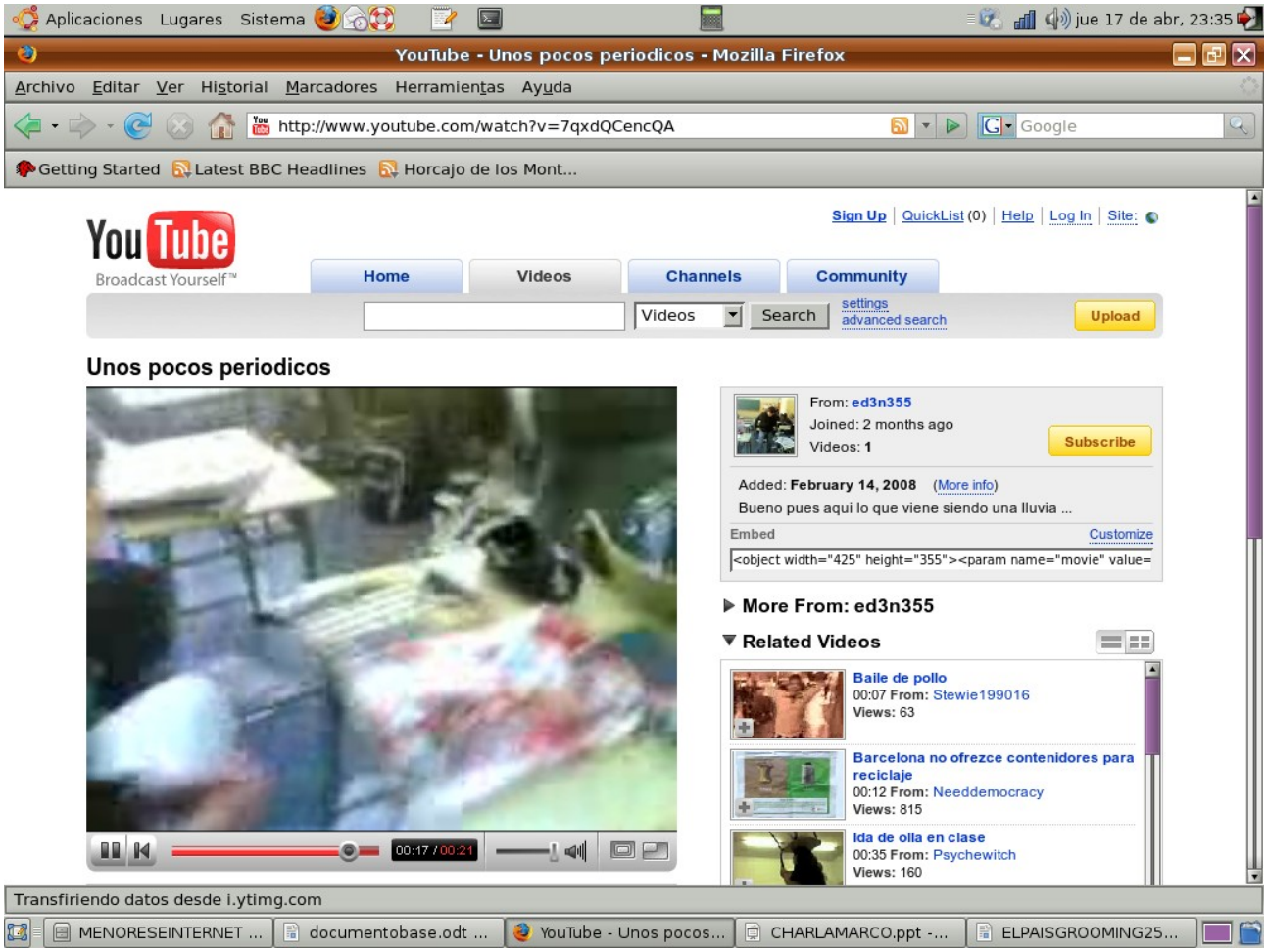
¿Cómo puede un malintencionado contactar con un menor de esta manera?. Desgraciadamente, existen varias maneras:

- Canales de chat
- A través de los programas de mensajería instantánea: no es tan difícil conseguir la dirección del "messenger" de un menor, partiendo de que son los propios niños los que dejan esos datos en determinados espacios como foros, blogs, fotologs, etc...

5.4. El acoso a través de las nuevas tecnologías. El "Ciberbullying".

Todos nosotros conocemos ya a través de los medios de comunicación el concepto de BULLYING, entendiendo como tal el acoso escolar que sufre un menor, normalmente a manos de otros menores, que se colocan en una posición de superioridad para agredirle física o moralmente de manera continuada, disminuyendo su autoestima y autoaceptación.

Este fenómeno, que todos sabemos que no es nuevo, ha tomado una nueva dimensión en el momento en que las tecnologías informáticas han proporcionado a los acosadores la posibilidad de ampliar la humillación proferida a sus víctimas propagando sus acciones.



¿Qué posibilidades nuevas abre a un acosador escolar el uso de las nuevas tecnologías?. Mencionemos sólo algunas:

- Grabar con el teléfono móvil la humillación (véase la ilustración superior) y propagarla enviándola a otros móviles, utilizando el correo electrónico o colgándola en espacios como Youtube
- Envío de mensajes SMS amenazantes o humillantes a la víctima
- Propagación de rumores a través de la red (usando canales como los foros, espacios web como los blogs tipo Blogger o Fotolog)

¿Cómo puedo saber si mi hijo está siendo objeto de acoso escolar en su entorno?. Desde la página institucional www.acosoescolar.info, se nos ofrecen las siguientes pistas:

Cambios en el estado de ánimo: parece triste.

Se muestra extraño y huidizo.

Parece nervioso; estado que se refleja en miedos nocturnos, micción en la cama, tics nerviosos, irritabilidad, etc.

Se muestra distraído, absorto en sus pensamientos, olvidadizo, asustadizo, etc.

Finge enfermedades o intenta exagerar sus dolencias: dolores de cabeza, de tripa, etc.

Presenta moratones, heridas, etc.

Rehúsa ir a la escuela, expone objeciones varias, simula malestar.

Falta al colegio y da explicaciones poco convincentes cuando se le pregunta el porqué o adónde fue.

No tiene amigos para su tiempo de ocio.

La manifestación de estas conductas no siempre se debe a situaciones de maltrato, por lo que es esencial charlar con nuestros hijos e indagar acerca de aquello que les puede estar ocurriendo. Aunque no siempre sea fácil charlar con un adolescente, pues sus cambios de humor, su deseo de intimidad y su rudeza en el trato -rasgos propios del proceso evolutivo por el que están pasando- hacen en ocasiones muy difícil la comunicación con ellos, los padres debemos emplear todas las estrategias posibles para hablar con ellos, si sospechamos que nuestro hijo está en situación de riesgo o padece maltrato.

6 PRINCIPIOS BÁSICOS DE SEGURIDAD

6.1. Adolescencia y familia

Cerraremos este documento enumerando un conjunto de normas muy sencillas de comprender, pero por lo mismo, bastante difíciles de aplicar, en algunas ocasiones, cuando tratamos con adolescentes. Siempre deberíamos partir de que ellos pueden tener más facilidad en la utilización de las tecnologías de la información y de la comunicación, pero somos nosotros los que tenemos una mejor perspectiva del mundo actual y de su funcionamiento.

El niño/adolescente se está enfrentando a multitud de cambios corporales, hormonales, psicológicos y sociales. Empieza a distanciarse del núcleo familiar que hasta el momento ha sido un pilar básico en su vida, dado que ya no puede ayudarle tanto en su evolución personal como el grupo de amigos, que empieza a convertirse en una referencia en cuanto a valores, objetivos y comportamiento.

Por otro lado, en muchas ocasiones es el propio adolescente el que busca el enfrentamiento con sus padres, como un modo de autoafirmarse y comprobar su capacidad y fuerza frente a la autoridad paterna. Resumiendo: cuando nuestros hijos entran en la "edad del pavo", hay broncas en casa un día sí y otro también.

Si añadimos al conjunto la intimidad que el niño empieza a guardar MUY celosamente, nos encontramos ante un cuadro bastante descorazonador. Queremos ayudarles, pero para ello necesitamos que nos escuchen y comprendan nuestro punto de vista. Es precisamente lo mismo que el adolescente espera de su familia, y reconozcámoslo: muchas veces tampoco ellos lo obtienen.

Releyendo estas líneas, me doy cuenta de que estoy expresando lo que quería, pero quizás pueda pintar un cuadro algo descorazonador para el padre de un adolescente. En realidad, empezar es bastante fácil. Sólo debemos tener claros algunos puntos:

- RARA VEZ EL ORDENADOR ES NECESARIO PARA ESTUDIAR: es cierto que colegios de primaria e institutos han incorporado la informática a su actividad diaria. Sin embargo, muy rara vez un profesor encargará a un niño una tarea para casa que exija soporte informático. Y en las contadísimas ocasiones en que ello suceda, el alumno puede aprovechar las propias instalaciones del centro educativo, así como cualquier cibercafé, biblioteca o asociación popular que siempre suele encontrarse cerca.
- LA COMUNICACIÓN CON NUESTRO HIJO ES IMPORTANTE: si nos preocupa el hecho de que el niño frecuente espacios en Internet como foros, chats... lo mejor es

preguntárselo directamente, y asegurarnos de que el niño conoce los peligros a los que se expone. En la adolescencia, el niño suele responder a la confianza que depositamos en él mejor de lo que nos esperamos. Si además, conoce las situaciones peligrosas que se pueden producir en estos casos, puede presentar una madurez semejante a la de un adulto.

- LA IGNORANCIA DE UN HECHO NO NOS PROTEGE DE SU REALIDAD: es mejor pasar por el mal trago de enterarnos de algo que no nos gusta que vivir en la inopia hasta que el asunto estalla en nuestras narices.
- EL HECHO DE QUE EL NIÑO TENGA MÁS CONOCIMIENTOS INFORMÁTICOS QUE NOSOTROS NO LE RESTA AUTORIDAD A NUESTRAS DECISIONES: las cosas se pueden negociar, contemporizar, consensuar... pero una vez hemos tomado una decisión, el niño debe plegarse a ella, le guste o no.

6.2. Decálogo de seguridad

Cerramos el presente documento orientativo ofreciendo una serie de consejos que deberían darnos algo más de tranquilidad (que nunca será absoluta) en lo relativo al uso que hacen nuestros jóvenes de la tecnología informática:

1. EL ORDENADOR DEBERÍA ESTAR EN UNA ZONA DE USO COMÚN DENTRO DE LA CASA.

Por muy celoso de su intimidad que se muestre nuestro hijo, no es inteligente permitirle tener una ventana abierta al mundo en su propia habitación, donde rigen sus propias normas y no podemos pasar con la libertad que deberíamos tener si pensamos que al fin y al cabo los dueños de la casa somos nosotros.

2. ES CONVENIENTE ESTABLECER UN HORARIO Y UNA SERIE DE NORMAS SOBRE LA CONEXIÓN A INTERNET.

El niño no debería poder conectarse cuando a él le de la gana. Al igual que con otras actividades diarias, debería ser consciente de que cuenta con un horario establecido para ello, fuera del cual no puede utilizar el ordenador. Por otro lado, deberíamos tipificar una normativa cuyo incumplimiento fuera sancionado con la desconexión de Internet. Ese tipo de castigos está demostrando ser más eficaz que otros tipos más tradicionales.

3. ES NECESARIO CONTAR CON UN BUEN PROGRAMA ANTIVIRUS.

Los problemas que hemos expuesto relacionados con la infección por un virus informático pueden ser atajados si contamos con un buen programa antivirus, legal, que esté adecuadamente actualizado (es decir, vaya siendo renovado diariamente a través de Internet para poder enfrentarse a las amenazas nuevas que surgen cada día).

4. TAMBIÉN ES NECESARIO CONTAR CON UN PROGRAMA CORTAFUEGOS (FIREWALL)

Un cortafuegos es un programa que controla las utilidades que tratan de conectarse a Internet, estableciendo una serie de permisos que tienen por objeto asegurar la seguridad del equipo informático que manejamos, cerrando el paso a cualquier pirata informático que trate de invadirnos mediante un troyano.

Si un programa ilegal trata de conectar nuestro ordenador al exterior sin nuestro permiso, el cortafuegos se lo impedirá y nos comunicará el hecho.

Actualmente, la mayoría de los programas antivirus tiene aparejada una utilidad cortafuegos.

5. DEBEMOS ASEGURARNOS DE QUE EL ADOLESCENTE CONOCE TODOS ESTOS PELIGROS.

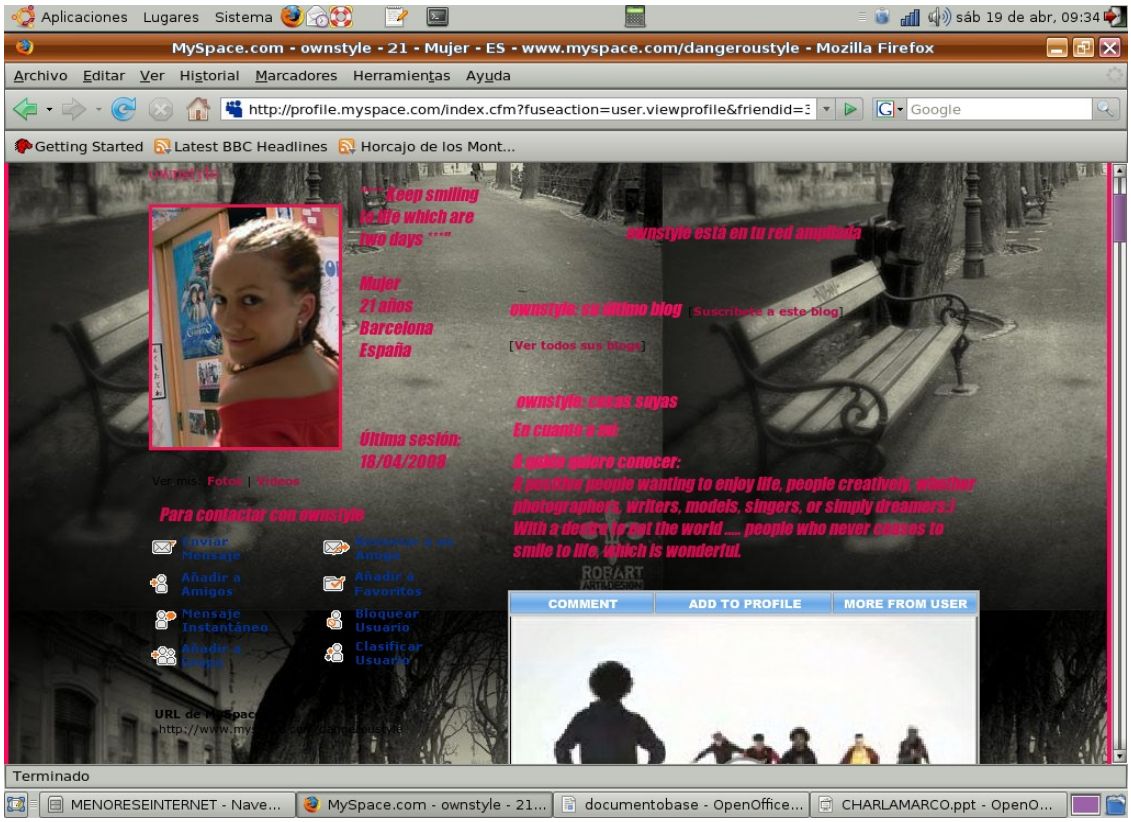
Como ya hemos adelantado, la ignorancia de un hecho que está sucediendo no nos protege de ello. Si un menor, con o sin nuestro permiso, accede, por ejemplo, a un servicio de chat, y contacta con otro usuario que muestra un comportamiento sospechoso o utiliza términos sexualmente explícitos o agresivos, podrá reaccionar de manera más adecuada que si no sabe lo que está pasando.

6. COMO NORMA GENERAL, EL MENOR NO DEBE DEJAR DATOS PERSONALES EN INTERNET BAJO NINGÚN MOTIVO.

En muchas ocasiones, deseamos acceder a servicios web (foros, páginas de descarga, etc...) que nos solicita previamente que nos registremos, dejando determinados datos, empezando por el correo electrónico. Esta práctica es lícita y normal, pero en ocasiones se nos piden otros datos como domicilio, número de teléfono, etc... con objetivos publicitarios o comerciales.

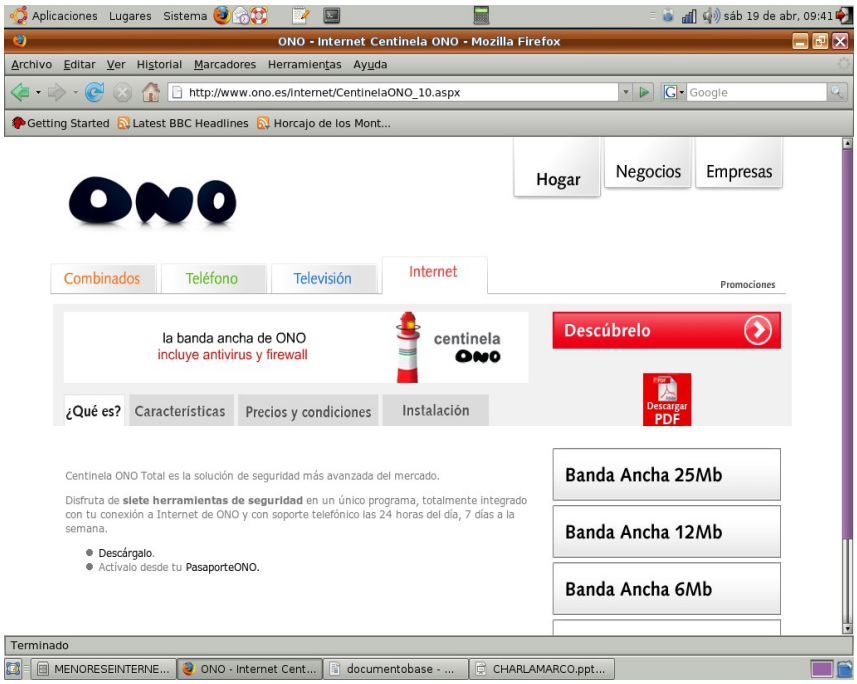
Además, ya hemos hablado de herramientas como los blogs, comunidades tipo MYSPACE, fotologs, etc... como de espacios que el niño utiliza para expresarse libremente, hablando de sus amistades, inquietudes, ilusiones, etc... pero donde debe moverse también con mucho cuidado para

no facilitar la invasión de su intimidad por parte de cualquier desalmado.



7. DEBEMOS INFORMARNOS SOBRE LAS HERRAMIENTAS DE PROTECCIÓN QUE FACILITE NUESTRO PROVEEDOR.

Muchos proveedores de Internet pueden facilitarnos algunas herramientas de protección al menor, que si bien según muchos internautas presentan errores de bulto en ocasiones, pueden resultarnos útiles. Estamos hablando de filtros como CENTINELA de ONO o CANGURONET de Telefónica, que de activarse desde Internet una vez nos hayamos identificado como clientes, pueden cerrar el paso a determinados contenidos en la red o facilitarnos algunas funciones simples como antivirus. Eso sí, es conveniente negociar durante la contratación de nuestra conexión que sean sus técnicos los que nos dejen el equipo informático preparado con dichas herramientas.



8. ES CONVENIENTE PRESCINDIR DE LA WEBCAM.

Una webcam, o cámara de vídeo conectada al ordenador, no tiene una utilidad fuera de la comunicación y el ocio, y podemos pasar sin ella. El objetivo de muchos degenerados, dentro de la práctica del CHILD GROOMING, es obtener imágenes del niño o niña mediante estos aparatos en una sesión de videoconferencia, para su propio uso y posteriores chantajes.

9. CUANDO APAREZCAN PROBLEMAS, EL NIÑO NO DEBE TEMER LA REACCIÓN DEL PADRE.

Insistimos en que la comunicación familiar es clave para garantizar la seguridad de nuestros hijos. Es lógico que si el niño se mete en un lío por algo que ha hecho rompiendo las normas, nos molestemos muchísimo, pero es imprescindible que el menor cuente antes con nuestro apoyo y protección ante cualquier amenaza que con una reacción de castigo.

10. COMUNICACIÓN CONTINUA SIGNIFICA PROTECCIÓN EFICAZ

Esta última regla de nuestro particular decálogo viene a complementar a la anterior. La adolescencia es un periodo problemático, confuso, en el que ya hemos dicho que el niño tiende a alejarse en cierto modo del núcleo familiar en busca de desarrollar un mayor grado de autonomía, acercándose más al grupo de amigos, y tendiendo a un comportamiento más hosco, incluso desafiante, en casa.

Sin embargo, y por mucho que a veces cueste esta comunicación, es muy importante que sigamos sabiendo qué hace el niño, en el ciberespacio y en la vida real, con quién pasa su tiempo, qué le preocupa y qué le ilusiona. Igualmente es importante que nuestro hijo sepa que puede seguir contando con nosotros, que seguimos ahí, apoyándole y dispuestos a ayudarle en todo lo que necesite.

Al fin y al cabo, nadie dijo que esto de ser padre ha sido fácil alguna vez, ¿no?.