GUÍA DE MENORES EN INTERNET PARA PADRES Y MADRES

PARA LOS PADRES Y MADRES

¿Qué ofrece Internet a los menores?

Del mismo modo que educamos a nuestros hijos en el uso de diferentes tecnologías (telefonía) o hábitos (buena educación) más arraigados en nuestra sociedad, Internet se ha convertido en uno de los pilares de la comunicación hoy en día y esto nos obliga a indicarles, desde pequeños, cuáles son las virtudes y los peligros de la red de redes, no solo porque es una herramienta imprescindible en su relación con el entorno social, sino que constituye una potente herramienta de educación y relación padres-hijos.

Pero del mismo modo que en la vida real, la red también es un lugar donde el menor puede encontrar información no adecuada y en ocasiones, se producen abusos.

Es por esto que aunque es normal que exista una lógica preocupación, no seria una actitud positiva mostrarse excesivamente restrictivo en su uso por parte de los menores, al contrario, se debe fomentar su uso de una manera segura.

Consejos generales.

1. Es necesario que los padres aprendan a utilizar el ordenador. De este modo y hasta cierta edad, se conectan con ellos y el niño aprende a disfrutar de Internet junto a sus padres; además conocer el ordenador ayuda a los padres a distinguir qué software utiliza y qué páginas visita el menor más fácilmente.
2. Fomentar el diálogo sobre hábitos de navegación y sus riesgos. Es importante que el menor sienta que cuando le suceda algo extraño para él o que le incomode pueda decírselo a sus padres sin sentirse culpable. Además les ayudaremos a mantener un espíritu crítico sobre la información que aparece en la red y les explicaremos que no todas las webs tienen la misma credibilidad.
3. Acordar unas normas de uso claras. Es particularmente bueno que los niños tengan reglas claras sobre lo que pueden o no hacer y conocer sus consecuencias, especialmente respecto al tiempo de uso (de día y no de noche, controlar su uso entre semana), de esta manera el niño sabrá a priori a lo que atenerse.
4. Es una buena ayuda utilizar filtros de control de acceso a la red. Así evitará que acceda a paginas de contenido inapropiado (adulto, violento, xenófobo, etc.). En el mercado existen soluciones gratuitas y muchos proveedores ofrecen soluciones de este tipo.
5. Es necesario colocar el ordenador en una zona de uso común. Facilitará la supervisión tanto del tiempo de uso (para controlar la ciberadicción) como el control de situaciones que puedan incomodarle, como por ejemplo, para evitar el ciberacoso cuando utilizan la webcam.
6. Enseñarles en qué consiste la privacidad. Explicarles que los datos personales son información sensible y que puede ser utilizada en su contra con ejemplos de la vida cotidiana, como puede ser, por ejemplo, que ellos nunca darían las llaves de casa a un desconocido o ejemplos similares.
7. Explicarles que en la red también hay que respetar a los demás. Que entiendan que detrás de un apodo, hay personas y que también hay que ser cortés y educado con ellas.

Consejos específicos según la edad de los menores.

De 4 a 12 años.

- Acompañarles en el uso del ordenador. A esta edad es imprescindible guiarles en el uso de esta tecnología.
- Conocer las claves de acceso. Ayudarles a escoger unas buenas claves de uso y explicarles la razón de esto.
- Enseñar los chavales a no descargar nada sin permiso: Muchas veces tienen la falsa creencia de que el nombre del archivo es indicativo del programa que están descargando, o en ocasiones descargan algo en el ordenador sin saber muy bien por qué lo han hecho.

De 13 a 18 años.

- Conocer los remitentes para no tener que leer los correos. A partir de la preadolescencia, los jóvenes son muy celosos de su privacidad, entonces se puede establecer un acuerdo intermedio en el que los padres conozcan las direcciones, al igual que el correo postal, pero no lean el correo electrónico -en el correo postal se puede leer el remitente, pero no es necesario abrir la carta-, y en el caso de que exista una dirección desconocida, es mejor preguntar al menor.
- Estar muy pendientes si se citan con algún desconocido. Insistirles en que no vayan solos, y que queden en un lugar público con más gente. Aleccionarles sobre que todo lo que se cuenta en Internet no tiene porque ser cierto.
- Enseñarles a tener un comportamiento responsable, respetuoso y ético en Internet. En muchas ocasiones tienen una falsa sensación de impunidad, que les hace atreverse con actitudes más agresivas, que en la vida real jamás adoptarían. Por esto, es recomendable explicarles que, cuestiones como el ciberacoso no puede ser divertido cuando se le hace daño o se molesta al prójimo.
- Asegurarse de que consultan antes de realizar cualquier transacción en línea. El comercio electrónico es cada vez más importante, es una buena enseñanza que se familiaricen con esta forma de comercio. No es necesario prohibirles que compren en Internet, pero sí es conveniente que consulten previamente a la introducción de datos bancarios de cualquier tipo.

SOBRE LOS MENORES

¿Qué problemas pueden encontrarse?

Un apartado orientado a las amenazas que puede encontrarse el menor y una guía para reconocerlas y evitarlas.

Virus y similares.

Los virus son pequeños programas que interfieren en el correcto funcionamiento del ordenador. Son muy variados y pueden producir muy diferentes efectos. Suelen detectarse como comportamientos no habituales del ordenador o pérdida de información.

Para evitar que los menores puedan sufrir la infección de un virus es muy importante disponer de un antivirus actualizado y cualquier fichero que se quiera tener en el ordenador (a través de un adjunto del correo electrónico, un disco USB portátil, un CD, etc.), hay que escanearlo previamente con el antivirus.

Privacidad del menor.

Se trata de un tema muy delicado, es muy importante mentalizar al menor sobre qué datos son de especial relevancia para la familia y para sí mismo y que no debe revelar en ningún caso sin la autorización de sus padres.

Del mismo modo, si el menor tiene una página web, un blog o similar es importante que esa mentalización se amplíe al respeto de dicho datos personales , incluyendo fotos y videos, porque si el menor, desconociendo la ley, hiciese un uso no autorizado de datos, imágenes o videos podría sufrir consecuencias legales importantes.

En la actualidad la privacidad está protegida por la Ley de Protección de Datos, que prevé importantes consecuencias en el caso de la violación de la privacidad.

Confianza en la Red.

Los menores suelen ser más crédulos que los adultos y como la mayoría de ellos ya han nacido con la existencia de Internet tienden a creer más en lo que ven en la red, incluso creen más que en los medios de comunicación tradicionales. Por este motivo hay que explicarles que en Internet no todo lo que se dice es verdad, ni todo lo que se ve tiene que ser real. Es necesario inculcarles un espíritu crítico respecto a lo que ven o les dicen por Internet, y que se acostumbren a verificar sus fuentes de información.

Contenido inapropiado.

No solo se trata del contenido sexual que pueden encontrar por la red, también pueden acceder a paginas de contenido violento o xenófobo, o incluso páginas con contenidos no adecuados a su edad y que ellos no son capaces de comprender, no porque sea inadecuado en sí mismo, sino porque no está adaptado a su edad. En este último caso la mejor recomendación es dirigirles a páginas en el que el contenido esté adaptado a su edad.

Consecuencias legales.

En los últimos años se ha legislado mucho de manera directa o indirecta sobre los diferentes usos de Internet, la tecnología cambia a toda velocidad y, en ocasiones cuesta seguir el ritmo de los cambios tecnológicos y legales.

A día de hoy, y en cuestiones que puedan afectar a menores de edad, las leyes más importantes respecto al uso de Internet son la Ley de Protección de Datos y la Ley de Propiedad Intelectual.

La Ley de protección de datos regula, entre otras muchas cosas, el uso que se hace de imágenes, datos personales o videos en la red, y estipula fuertes multas en el caso de que se invada la privacidad de una persona.

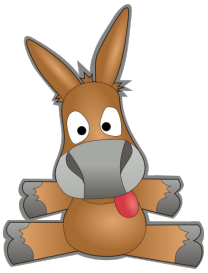
Por otro lado, la ley de propiedad intelectual indica que los programas de ordenador (aplicaciones y juegos) pirateados son delito y prevé fuertes multas por ello.

El software pirateado son aquellos programas no gratuitos que se utilizan sin haber pagado una licencia o habiéndose saltado la protección que tengan.

¿Qué suelen hacer ellos en Internet?

Estabas navegando, y siguiendo algún enlace te has encontrado con alguna pagina para adultos, sobre violencia o racismo, o cualquier otra que te haya hecho sentir mal.

Uso de las redes p2p.



Estas redes son en la actualidad uno de los más importantes usos que se da a Internet, y se ha generado una fuerte controversia en torno a su uso para la descarga de contenidos protegidos por derechos de autor.

Para evitar problemas de seguridad y legales en el uso de estas redes, es importante concienciar a los menores en que no confíen en que el nombre de los ficheros que aparecen no tienen porque indicar el contenido y en muchas ocasiones pueden contener virus, para ello es importante que todos los ficheros que se descarguen a través del p2p los escaneen previamente a su uso con un antivirus actualizado. También es importante explicarles las consecuencias legales de la descarga de software (juegos y aplicaciones)

Chat, mensajería instantánea.

En la actualidad el uso de la mensajería instantánea[1] se ha generalizado entre los jóvenes y constituye uno de sus principales medios de contacto con amigos y conocidos en todo el mundo.

Existen dos amenazas a través de esta tecnología: que adultos aprovechen la facilidad para ocultar la identidad real y la confianza de los menores para intentar engañarles, y la dispersión de virus a través del envío de enlaces maliciosos.

La primera amenaza se podría minimizar explicándoles que no deben citarse con alguien que hayan conocido a través de la red, y si lo hacen que lo hagan en compañía de más gente y en un lugar público y haciéndoles comprender que en internet no todo es lo que parece.

1 Esto se refiere a los programas como el Windows Live Messenger, el ICQ, Pidgin, GTalk o Yahoo! Messenger

Navegación por Internet.

El uso generalizado de Internet es una de las grandes revoluciones de principios de este siglo, fomentar su uso en todas las disciplinas es una de las aspiraciones de la educación actual, pero estas cuestiones tan positivas deben acompañarse de una educación sobre lo que significa la privacidad y la confiabilidad que permita a los menores construir un criterio sobre la navegación segura.

Además los padres y madres deben fomentar un diálogo abierto sobre los contenidos más adecuados para la edad de los menores y enseñarles que existen contenidos que solo deben ser para adultos.

Internet es como una biblioteca gigante, se puede encontrar toda la información que te puedas imaginar, pero existen páginas que no tienen buenas intenciones cuando te ofrecen cosas.

Procura siempre tener varios programas de protección del ordenador para que puedas navegar con la máxima tranquilidad.

Cuando, por casualidad, llegues a una pagina que no entiendes o te sientes mal con lo que pone, no tienes por qué seguir en esa página, la cierras, no vuelves a esa página y ya está, y si tienes alguna duda, le preguntas a tus padres.

Uso del correo electrónico.

Aunque los menores no tienen entre sus preferencias el uso del correo electrónico, sería positivo que adquiriesen una serie de hábitos de seguridad sobre la utilización de esta tecnología porque probablemente su uso vaya aumentando con el tiempo.

Para ello es importante que:

- Tengan dos cuentas de correo electrónico.
- Una para dársela a tus familiares y amigos y otra para registrarte en foros, redes sociales o juegos en línea.
- Que no contesten correos de personas que no conocen.
- Esos correos deben eliminarlos, se tratan de engaños que incluso pueden contener un virus.
- Explicarles que por Internet circulan una gran cantidad de bulos (en ingles, hoax).

Que se han convertido en autenticas leyendas urbanas, y hay mucha gente que se los cree, decirles que es mejor que no ayuden a aumentar la mentira porque pueden perjudicar a mucha gente. Cualquier correo de este tipo que reciban es mejor que busquen otras fuentes de información para asegurarse de que es verdad.

- Que no descarguen archivos adjuntos si no están seguro sobre de quién es el mensaje.

Y si lo saben, después de descargar el adjunto, que le pasen un antivirus antes de abrirlo.

Foros.

En estos lugares suelen consultar la mayoría de las dudas informáticas o no, que suelen tener, las recomendaciones de uso son muy similares a las de la mensajería instantánea.

Juegos online.

Debido a la mejora de las conexiones, cada vez aparecen más páginas en las que los menores pueden jugar en línea con otros usuarios de todo el mundo. Las recomendaciones generales son las mismas que en el caso de la mensajería instantánea, ya que estos juegos suelen tener un chat para que los jugadores puedan comunicarse entre sí.

Específicamente se recomienda que el software que está instalando en el ordenador para jugar en línea este actualizado con los últimos parches de seguridad y que no instalen parches que no sean oficiales, porque con bastante frecuencia suelen tratarse de virus.

Redes sociales.

Son el ultimo "boom" en Internet. En estas redes se relacionan con sus amigos, conocenamuchagenteysuelendar,conmucha confianza, muchos datos personales.

La redes sociales son una buena ayuda para la socialización del menor, por ello, hay que apoyar que las utilicen, pero hay que inculcarles el criterio de que elijan muy bien a quién agregan como amigo, porque ese amigo va a tener sus datos personales y estos datos pueden ser utilizados en su contra.

Consejos generales para el mantenimiento del equipo

El sistema operativo.

Es el corazón del software del ordenador, y es necesario tener actualizado, por lo que es recomendable tener activadas las actualizaciones automáticas.

El software de protección.

Sirve como ayuda para evitar al menor en los posibles incidentes de seguridad que se pueden dar utilizando Internet (infección de un virus o de algún programa espía, etc.), para ello es importante tener instalados y actualizados programas que sirvan para proteger el ordenador y el menor de estos incidentes. Existen muchos tipo de software de protección, pero de manera general podemos clasificarlos en tres grupos.

- **Antivirus**: Software que sirve para evitar las infecciones por virus y otros tipos de malware o programas maliciosos como gusanos, troyanos, etc.
- **Antiespías**: Estos programas evitan la ejecución de programas espía (también conocido como spyware) y que puedan robarles información sensible a los menores.
- **Cortafuegos**: Son programas que controlan la comunicación entrante y saliente de y hacia Internet, de esta manera se evita que pueda salir información sin que el usuario del ordenador se entere, o que otro ordenador establezca conexión con el nuestro sin consentimiento.

Asimismo también existen herramientas de control parental, que sirven para restringir y monitorizar el uso que hace el menor de Internet, son herramientas que suponen una intrusión en la intimidad del menor y aunque son perfectamente legales, a partir de ciertas edades se recomienda que su uso, si fuese necesario, se consensue con el menor.