Aquí tendes unha relación de consellos para os pequenos internautas, para os pais e para os usuarios de Internet en xeral, que nos enviou o axente da Garda Civil que nos deu a charla sobre seguridade na rede.

Consejos para pequeños internautas

1. **No des nunca tu nombre, no digas donde vives ni como se llaman tus padres, no envíes fotografías tuyas ni de tu familia. No informes de tu horario de colegio ni de quien te va recoger.**
2. **Si alguien te dice algo que te resulta incómodo o molesto díselo rápidamente a tus padres.**
3. **No quedes nunca con nadie que hayas conocido en Internet sin el conocimiento y la autorización de tus padres.**
4. **Nunca compres nada por Internet sin el conocimiento y consentimiento de tus padres.**
5. **No te descargues programas, música, películas, ni videojuegos sin el conocimiento de tus padres, aunque la página diga que es gratuito. Algunos de estos ficheros contienen contenidos para adultos o programas ocultos que pueden dañar tu ordenador y espiar tu navegación.**

Consejos para padres

LA SOCIEDAD DE LA INFORMACIÓN SE CARACTERIZA POR EL USO DE NUEVAS TECNOLOGÍAS QUE EVOLUCIONAN A RITMO DE VÉRTIGO. NO TODOS LOS CIUDADANOS ACCEDEN A ESAS NUEVAS TECNOLOGÍAS A LA MISMA VELOCIDAD NI SE ADAPTAN IGUAL. POR NORMA GENERAL, NUESTROS MENORES SABEN MÁS INFORMÁTICA QUE LOS ADULTO, SIN EMBARGO CARECEN DE LA EXPERIENCIA Y MADUREZ PARA DETECTAR PELIGROS. PODEMOS ENSEÑARLES A ESTAR PREVENIDOS FRENTE A LOS RIESGOS DE INTERNET E INCULCARLES HÁBITOS DE NAVEGACIÓN SEGURA Y DENTRO DE LA LEY.

1. **Internet y la informática ofrecen numerosas ventajas. Por ello, debemos animar a nuestros hijos en el uso de estas tecnologías, pero no en el abuso. Limite las horas que sus hijos dedican a estar frente al ordenador o conectados a Internet. Procure supervisar los contenidos a los que accede.**

2. **Existen contenidos en Internet sólo aptos para personas adultas o con una adecuada formación intelectual y moral. Existen programas que filtran el acceso a determinados contenidos. Si considera**

que su hijo no está preparado para entender esos contenidos, utilice esos programas. No escatimemos costes en la educación de nuestros hijos.

3. **Internet también ofrece riesgos. El fraude y la provocación sexual son los principales riesgos a los que sus hijos se pueden enfrentar. Insístales en que no deben proporcionar datos personales, ni nombre, ni direcciones ni horario de colegios. No debe establecer citas reales con nadie sin su conocimiento.**

4. **Alerte a su hijo del riesgo de intimar por Internet con personas desconocidas. La mayoría de las veces, dista mucho lo que se dice ser de lo que realmente se es. Los servicios de mensajería instantánea como el popular "Messenger", permite contactar con multitud de personas y abrir el círculo de relaciones. No establezca comunicaciones con aquellos de los que no tiene una referencia en la vida real (conocidos por terceros).**

5. **Si su hijo le informa de contenidos que le han hecho sentir incómodos (de tipo sexual) déle la importancia que realmente tiene y denúncielo.**

6. **No permita que su hijo efectúe él solo compras a través de Internet. Supervise Vd. las compras.**

7. **Eduque a su hijo sobre las consecuencias negativas de vulnerar las leyes de propiedad intelectual. El que "mucha gente lo haga" no implica que sea legal. Respetemos los derechos de propiedad intelectual que ayudan y permiten una industria que fomenta la creatividad y enriquece nuestra cultura. La piratería digital tiene como mejor solución la educación ciudadana en el respeto a los derechos de los demás.**

Consejos para usuarios de Internet

Actualice constantemente el sistema operativo y el software instalado, especialmente el navegador web. Los sistemas operativos y la mayoría de los programas

utilizados tienen una función configurable de actualización (*update*) automática. Actívela.

Si utiliza sistemas Windows, trabaje con una cuenta de usuario que no tenga privilegios de administrador. De esta forma evitará la posibilidad de instalación de muchos programas maliciosos.

Utilice un software antivirus. Mensualmente se generan más de 1.000.000 de programas maliciosos tipo *malware* (software malicioso). Las empresas antivirus actualizan diariamente sus listados para hacer efectivo su servicio. Es preciso que nuestro antivirus se actualice periódicamente. Rehúse copias piratas.

Instale un programa cortafuegos o *firewall*. En la red hay multitud de estas aplicaciones. Algunas de ellas gratuitas y de contrastada eficacia. No le preocupe no tener el mejor, preocúpele no tener uno instalado.

No abra mensajes de correo electrónico no solicitados o de procedencia desconocida. Elimínelos directamente sin previsualizarlos.

Tenga especial cuidad con las redes P2P (per to per). Es una de las más importantes fuentes de infección de *malware*. Analice con su antivirus todo lo que se descarga.

Cuando navegue por Internet, busque páginas de confianza, a ser posible, avalados por sellos o certificados de calidad, evitando contenidos dudosos. Su exigencia de calidad ayudará a lograr una Internet más segura

Utilice siempre software legal. Evita las descargas de programas de lugares no seguros de Internet.

Si recibe mensajes que piden el reenvío a sus conocidos, informando de noticias llamativas o apelando a motivos filantrópicos, desconfíe por sistema. Muchos de ellos buscan captar direcciones de correo electrónico para prospectivas comerciales, y son un engaño (*hoax*).

Desconfíe de los mensajes de correo procedentes de supuestas entidades bancarias. Confirme vía telefónica, en su sucursal bancaria, cualquier petición que reciba de datos de banca electrónica.

En las redes sociales, limite el acceso de la información que comparte a personas conocidas (mis amigos). Cuando más amplio sea el círculo de contactos (amigos de mis amigos y todos los usuarios), a más riesgos se expone.

LA ADOPCIÓN DE ESTAS MEDIDAS NO GARANTIZA LA SEGURIDAD DE NUESTROS SISTEMAS PERO REDUCE EN UN 90% SU VULNERABILIDAD.

LOS SISTEMAS INFORMÁTICOS ALMACENAN INFORMACIÓN CONFIDENCIAL. NO RENUNCIEMOS A NUESTRA INTIMIDAD INVIRTAMOS EN MEDIDAS DE SEGURIDAD PARA NUESTROS SISTEMAS INFORMÁTICOS.