

Con motivo de la celebración del Día Mundial de Internet el 17 de mayo

La AEPD apela a la responsabilidad de los usuarios en la web 2.0 y a la protección de los menores en una nueva guía con recomendaciones sobre Internet

- La AEPD recuerda la necesidad de respetar los derechos de los demás cuando se utilicen aplicaciones que permiten publicar datos personales videos o fotos.
- Se incluye un apartado específico sobre el uso de Internet por los menores, recalcando la importancia de educarles en un uso seguro de Internet y de adoptar medidas de seguridad.
- La Guía recoge 12 campos de la Red en los que los usuarios pueden estar expuestos a riesgos -como las redes P2P, los buscadores, las videocámaras en Internet y las redes sociales- y aporta recomendaciones para prevenirlos.
- Recoge un glosario con vocabulario relacionado con el entorno de Internet, que puede resultar de utilidad para los internautas.

(Madrid, 13 de mayo de 2009). El domingo 17 de mayo se celebra el quinto aniversario del **Día Mundial de las Telecomunicaciones y Sociedad de la Información** –también conocido como el **Día de Internet**- una iniciativa que tiene como objetivo **difundir y promover el uso de Internet en la sociedad**.

Para la Agencia Española de Protección de Datos, miembro del Comité de Impulso del Día de Internet, resulta prioritario crear en la ciudadanía una **cultura para la protección de sus datos en Internet**, y por este motivo ha elaborado una nueva **Guía de Recomendaciones a Usuarios de Internet**.

La publicación está **estructurada en 12 apartados** en los que se analizan los principales **riesgos** que aparecen actualmente en la red y se enumeran algunas **recomendaciones para tratar de prevenir sus efectos**. Además, en esta nueva edición de la Guía para usuarios de Internet, que refleja las nuevas realidades de Internet, como las redes sociales o videocámaras en Internet, **se destaca especialmente la necesidad de proteger a los menores en la Red, y se apela a la responsabilidad de los internautas en el entorno de la llamada web 2.0., ante las posibilidades de difusión de información personal -datos o fotografías y videos- propios y de terceros que ofrecen servicios como redes sociales o blogs**.

Entre las recomendaciones contenidas en la guía, cuyo contenido íntegro está disponible en www.agpd.es, cabe destacar las siguientes:

La responsabilidad de los internautas

La evolución de Internet por la cual los usuarios han pasado de tener un papel pasivo a uno activo, ha supuesto la aparición de aplicaciones que permiten publicar informaciones, videos o fotos, en las que podemos estar mostrando datos personales de

terceros, sin tener en cuenta los perjuicios que se pueden ocasionar. De ahí la necesidad de ser conscientes de nuestra responsabilidad, personal y jurídica. Es aconsejable:

- No publicar informaciones que no respondan a los requisitos de veracidad, interés público y respeto a la dignidad de las personas. No difundir rumores.
- No grabar ni publicar imágenes, videos o cualquier otro tipo de registro sin el consentimiento de los afectados.
- Tener especial cuidado al publicar información relativa a los lugares en que el usuario o un tercero se encuentra en todo momento. Podría poner en peligro a los usuarios.

Asimismo, se recomienda a responsables de los portales de Internet que permiten estas actividades:

- Rectificar o retirar la información cuando lo solicite un afectado de modo justificado.
- Informar sobre los deberes de los usuarios en los procedimientos de alta y registro.
- Elaborar y publicar códigos éticos que garanticen unas mínimas reglas de actuación de los usuarios o de las comunidades en las redes sociales.

Uso de Internet por menores

- Los niños son nativos digitales, usan Internet como parte normal de su vida. Debemos educarles en un uso seguro de las redes.
- Aprenda a usar las herramientas de Internet y a navegar con sus hijos con la finalidad de educarles.
- Adopte medidas de seguridad físicas -ubicación del ordenador, horas para su uso- e informáticas.

Las redes sociales

- Las redes sociales son una importante fuente para la obtención de información sobre las personas. Debe conocer bien su funcionamiento para proteger su identidad digital.
- Debe garantizar la seguridad de su información mediante una configuración adecuada de su perfil y utilizando contraseñas adecuadas.
- Cuando publica una foto o escribe en un foro puede estar incluyendo información sobre otras personas. Respete sus derechos.

Los buscadores

- El uso de un buscador genera tratamientos de información como mínimo para ofrecer anuncios personalizados. Conozca las políticas de uso de su buscador preferido.
- Recuerde borrar con regularidad las cookies, los archivos temporales de Internet, así como el historial de navegación.
- Los buscadores permiten a cualquier tercero obtener perfiles completos sobre nuestra información pública en Internet.

Las videocámaras en Internet

- La imagen es un dato de carácter personal cuya difusión o acceso no autorizado puede ser particularmente molesto o dañino.
- Antes de instalar una videocámara que reproduzca imágenes en Internet, asegúrese de que la captación sea lo menos intrusiva posible.
- Debe garantizarse la seguridad impidiendo el acceso no autorizado a las imágenes captadas por cámaras IP.

Correo electrónico

- Cuando envíe mensajes de correo a una variedad de destinatarios, utilice el campo "*Con Copia Oculta (CCO)*".
- Para acceder a su cuenta de correo electrónico, además de su código de usuario utilice una contraseña.
- No utilice la opción de "*Guardar contraseña*" que en ocasiones se le ofrece, para evitar reintroducirla en cada conexión.
- Active los filtros de correo no deseado de su programa de correo electrónico.
- No proporcione su dirección de correo electrónico si no está seguro de las intenciones de quien la requiere y evite difundir las direcciones de otras personas.

Los servicios *Peer to Peer*

- Es conveniente la instalación de un "cortafuegos" que proteja del acceso no deseado al propio ordenador.
- Es preferible no descargar programas ejecutables o ficheros que sean susceptibles de contener "software malicioso".
- Nunca comparta todo su disco duro. Use un disco duro dedicado en exclusiva o establezca una carpeta o directorio específico.
- Deberá valorarse la idoneidad de restringir el uso de estos sistemas en los centros de trabajo, dado el riesgo de que se pueda llegar a compartir información de terceros.

Virus, gusanos y ataques de Ingeniería Social

- Sea cuidadoso con los programas que instala.
- Añada programas "cortafuegos" y de detección y eliminación de "software espía".
- No proporcione información sobre sus identificadores de usuario y mucho menos sobre sus claves de acceso.

Comercio y Banca electrónica

- Antes de aportar ningún tipo de datos personales debemos asegurarnos de que se ha establecido una conexión segura con el portal.
- Desconfiar de los correos electrónicos que informan de cambios en las políticas de seguridad y solicitan datos personales y claves de acceso.

Servicios de mensajería instantánea y chats

- El nick no debe proporcionar información personal.
- No facilitar datos que puedan afectar a nuestra intimidad, nombres de pantalla o direcciones de correo electrónico a interlocutores no conocidos.

Navegación por Internet

- Actualizar periódicamente el "software antivirus" y de seguridad, así como configurar el software del navegador con las opciones de seguridad más restrictivas.
- El intercambio y la entrega de datos de carácter personal deberá efectuarse en los sitios web que dispongan de protocolos seguros y de política de privacidad.