Desarrolla

PantallasAmigas desde 2004

Impulsa

Telefónica

PILAR Y SU CELULAR

HISTORIAS PARA CONTAR

WWW.PILARYSUCELULAR.COM

~ INSTALANDO APPS ~

JUSTIFICACIÓN

La cantidad de apps que podemos instalarnos crece exponencialmente. Algunas de ellas son atractivas o útiles, otras no lo son tanto, pero todas ellas pueden acabar instaladas en nuestro teléfono inteligente. Son, al fin y al cabo, programas informáticos que metemos en nuestro ordenador de bolsillo conectado a Internet que guarda y registra toda nuestra actividad (con quién hablamos, qué escribimos, dónde estamos…) e información. Las apps durante el proceso de instalación solicitan permiso para acceder a este diario y fichero que tenemos, sin que seamos conscientes, en el smartphone.

HISTORIA

2'12" MIN.

Pilar decide instalar una nueva app que en apariencia es muy atractiva "Secret Chat". Durante el proceso de instalación la app solicita que Pilar le conceda acceder a diversos datos que su Smartphone puede proporcionar: ubicación, imágenes, contactos… Ella no reflexiona mucho, tampoco está segura de entender lo que significan esos avisos, pero a pesar de todo decide dar una vez más al botón de aceptar para que el proceso de instalación se complete y empezar a disfrutar cuanto antes de la nueva aplicación.

Autores: Jorge Flores Fenández - Urko Fernández Román

FICHA

Ámbito Privacidad.

Temática Cesión de datos.

Texto en la entrada

¿Sabes qué datos personales cedes al instalar una app?

Texto en salida

1 Existen apps que no respetan tu vida privada (fotos, datos…)

2 Evita instalar apps que usen tus datos sin necesidad o sin explicar para qué los utiliza.

Mensajes principales

- Es importante conocer qué permisos concedemos a las apps que instalamos en el celular.
- Saber qué significan los permisos de privacidad es el primer paso para evaluar la pertinencia de concedérselos a una nueva app.

Mensajes complemetarios

- El smartphone es un completo computador que gestiona y almacena gran cantidad de información privada y que está conectado a Internet.
- Existen apps que han sido creadas exclusivamente para recopilar los datos de los celulares en las que están instaladas y que la función o servicio que ofrecen es una mera excusa.
- Para evaluar una app puede ser útil buscar qué opinan otras personas de ella antes de instalarla. Google puede ayudar en esa labor también.

Otras reflexiones a reforzar

- Aunque no se oculte nada importante en el celular nadie tiene derecho a acceder a lo que en él se guarda.
- Puede que otras personas consideren importante la información que comparten cuando se comunican con alguien y no quieran que sea tomado por ningún programa sin una causa justificada.
- Son muchas las informaciones que almacenadas en el teléfono celular de las que ni siquiera nos damos cuenta.

Preguntas para provocar la conversación

- ¿Cuál es la app de tu celular que más utilizas?
- ¿Alguna vez al instalar una app te has parado a leer los permisos de acceso a tu celular que solicita?

Datos de interés

- En el mes de febrero del pasado año 2015 hubo 260.000 nuevas versiones de apps o nuevas apps en Google Play.
- En el mismo mes, 42.000 apps desaparecieron porque las retiró su creador o porque Google las expulsó por realizar alguna acción que incumpliera las normas del market. (fuente: Path 5, http://bit.ly/1PxY5df)

ACTIVIDAD PROPUESTA 1

Objetivos | Reflexionar sobre los permisos que solicitan las apps (acceso a la ubicación, agenda, mensajes, archivos multimedia...)

Lugar | Preferiblemente en el centro escolar, pero también en el hogar.

Divididos en grupos de cinco, cada grupo escogerá de entre las aplicaciones que más frecuentemente utilicen, las tres más populares. Cada grupo indicará por cada app seleccionada, qué permisos son requeridos a la hora de instalar y/o usar la herramienta y, por cada permiso que se identifique, qué tipo de datos personales son accesibles por la app (indicando algunos ejemplos), qué uso hace la app de esos datos, si los datos serán visibles en Internet por terceras personas, si es posible que la app funcione sin otorgar ese permiso en concreto y si están de acuerdo o no en que esa aplicación solicite ese permiso.
De forma colectiva se reflexionará acerca de aquellas aplicaciones que coincidan en más de un grupo, aclarando con detenimiento el acceso y uso no apropiado a los datos personales y, por ende, a la vida privada, que realicen esas apps.

ACTIVIDAD PROPUESTA 2

Objetivos | Explorar la forma en que la información puede llegar a salir de las herramientas móviles y hacerse pública para todo Internet.

Lugar | Preferiblemente en el hogar, pero también en el centro escolar.

Partiendo de una app que tanto hijos e hijas, como padres y madres utilicen en común (Whatsapp, Facebook, Instagram, YouTube....), cada grupo generacional buscará a través de algún buscador popular (Google, Yahoo, Bing...) datos personales del otro grupo hasta encontrar cinco de ellos. Además de los datos personales tradicionales (nombre, apellidos, número de teléfono, número de identidad, lugar de nacimiento, edad, domicilio...) también se podrán encontrar fotografías que fueron compartidas de forma privada.

La actividad consiste en que una vez se encuentren los datos personales, se reflexione acerca de si deberían estar accesibles públicamente y, de no ser así, tratar de eliminarlas de Internet o configurarlas para que no sean accesibles de forma pública.

Recomendaciones para una parentalidad digital positiva

- Interésate por las app que tus hijos e hijas utilizan, pídeles que te ayuden a instalar algunas de ellas y te enseñen a utilizarlas. Procura buscar espacios para compartir momentos en familia a través de esas apps sin que resulte forzado ni obligado.
- Investiga en foros, páginas web o canales de YouTube especializados si una app es recomendable para ser usado por niñas, niños o adolescentes incidiendo especialmente en la forma en que esa app afecte a su vida privada.
- Respeta la privacidad de tus hijos e hijas procurando no invadir los espacios de intimidad que hayan creado con sus amistades a no ser que se hayan detectado problemas y no hayan sido capaces de compartirlos. Invadir su privacidad debe tener una causa justificada y una decisión muy meditada.