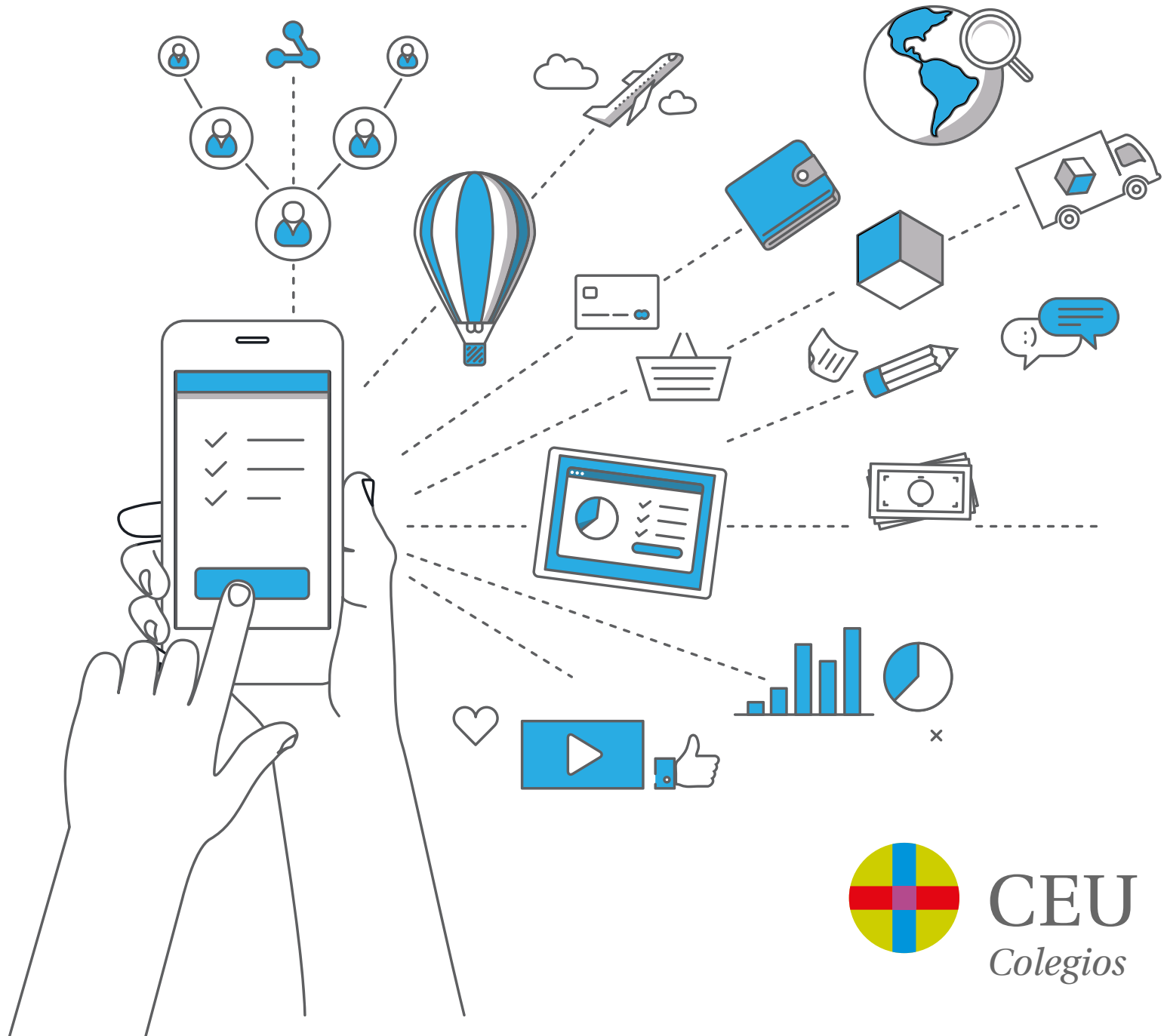
Familias conectadas

Guillermo Cánovas

40 preguntas sobre internet

que te harán tus hijos



CEU Colegios

Guías Familias Conectadas

40 preguntas que tus hijos te harán sobre internet

Queridas familias:

Cada vez somos más conscientes de la importancia de educar en el uso de las nuevas tecnologías y de la necesidad de formarnos al respecto. Todos percibimos que el avance tecnológico es vertiginoso y, en este sentido, muchas veces podemos vivir situaciones personales o familiares ante las que no sabemos qué hacer o cómo actuar.

Por este motivo y para facilitaros más formación en este ámbito, desde el Área de Colegios CEU hemos elaborado la presente guía “40 preguntas sobre internet que te harán tus hijos” junto con Guillermo Cánovas, Director del Observatorio para la Promoción del Uso Saludable de la Tecnología.

Creemos que os puede ayudar a tener pautas y a dar respuesta a muchas de las cuestiones que vuestros hijos os pueden plantear. Queremos que las familias también seáis un referente en estos temas y, como siempre, desde los colegios CEU, os queremos continuar acompañando en vuestra tarea educativa.

Esperamos que sea de vuestro interés.

Recibid un cordial saludo.

Raül Adames

Director Área Colegios CEU

GUILLERMO CÁNOVAS

PERFIL DEL AUTOR

Director del Observatorio para la Promoción del Uso Saludable de la Tecnología “Educalike”.

Director del Centro de Seguridad en Internet para los Menores en España, integrado en el Safer Internet Programme de la Comisión Europea (2002-2014).

Profesor y escritor.

RECONOCIMIENTOS

Premio UNICEF en 2013.

Condecorado con la Cruz de la Orden del Mérito.

LIBROS

Autorregulación Digital | Cariño he conectado a los niños | Adolescencia y drogas de diseño | Acoso Escolar | Adolescentes y alcohol... y otros.

INTRODUCCIÓN

A lo largo de los últimos veinte años he tenido miles de sesiones formativas con alumnado de 8 a 18 años. Una parte de cada sesión se dedica a algo muy importante: resolver sus numerosas dudas. Se trata de preguntas que formulan sobre cuestiones que les inquietan, relativas a su privacidad, su seguridad, sus derechos y también sus obligaciones. Cuando esto sucede es por una razón muy clara: no las formulan en casa. Es necesario que en la familia seamos un referente también en estos temas, y que puedan preguntarnos cualquier cosa al respecto.

Ese es el objetivo de esta guía, con preguntas que surgen habitualmente:

Cuando subo mis fotos a una red social, ¿pueden utilizarlas si quieren?

Cuando me llega una noticia al móvil, ¿cómo puedo saber si es falsa -fake news-?

¿Con cuántas horas de uso de internet al día se puede considerar que tengo una adicción?

Si utilizo un nombre inventado cuando me creo una cuenta en internet, ¿puedo estar cometiendo un delito?

¿Puedo publicar una foto de mi cumpleaños con mis amigos si tengo su permiso?

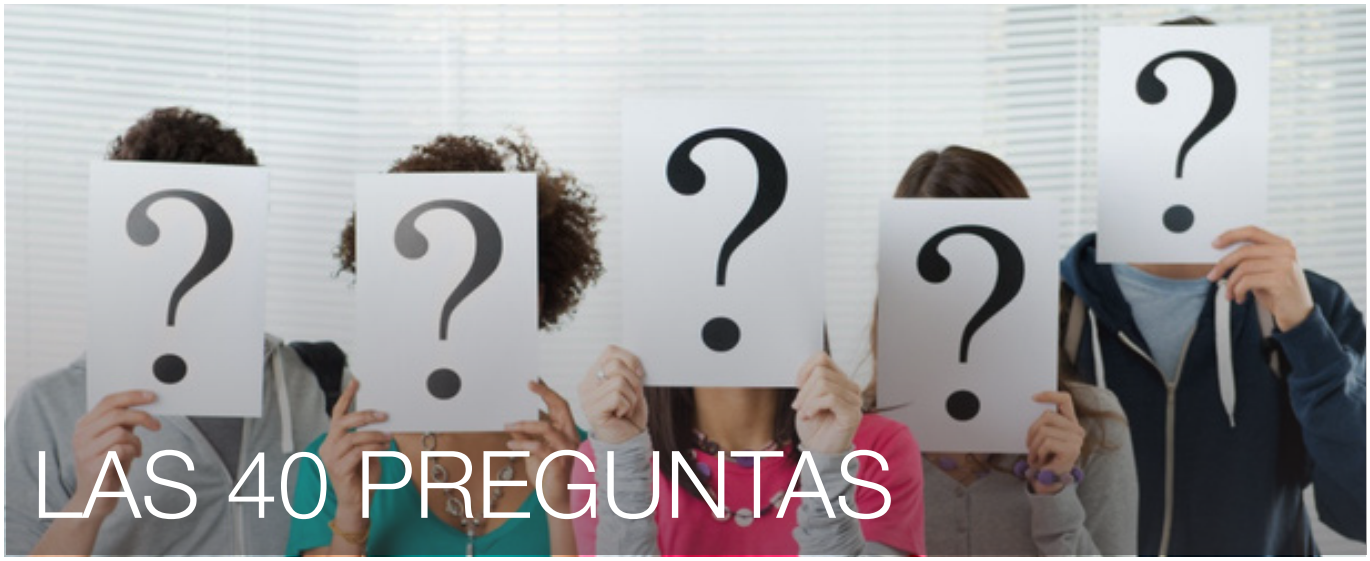
Cuando hago una búsqueda en Google ¿me puedo fiar de los resultados?

Cuando me desinstalo una aplicación, ¿pueden seguir accediendo a los contenidos de mi móvil o tableta?

¿Puedo ponerme de foto de perfil, la foto de un famoso que he encontrado en internet?

... y 32 preguntas más.

CEU Colegios



LAS 40 PREGUNTAS

1.Cuando subo una foto o vídeo a una red social, ¿pueden utilizarla si quieren?

Este es uno de los problemas que surgen cuando no leemos los términos y condiciones de uso, y los permisos que nos solicitan las aplicaciones que instalamos en el móvil o la tableta. Esos permisos incluyen todo tipo de cuestiones que deberíamos tener muy en cuenta antes de aceptar. Muchas herramientas, entre ellas las redes sociales, notifican que al crear una cuenta les **otorgamos una licencia de uso no exclusiva, a nivel mundial y de forma gratuita, para que utilicen nuestras fotos o vídeos.** Así sucede en Instagram, TikTok, Twitter, Facebook y otras.

2. Cuando me llega una noticia al móvil ¿cómo puedo saber si es falsa (fake news)?

La difusión de información y noticias falsas es un fenómeno que crece de manera exponencial. Se produce sobre todo a través de mensajes en las redes sociales o de sistemas de mensajería instantánea como Whatsapp. Difundirlas puede acarrear consecuencias de distinto tipo a las personas que las reenvían a sus conocidos y amistades. Pueden generar problemas de relaciones, hacer que pierdan credibilidad, perjudicar a otras personas o incluso provocar problemas emocionales tal y como señalan diversos estudios sobre el tema.

Estas informaciones falsas pueden ir acompañadas del logo de algún reconocido medio de comunicación, para intentar engañar a los lectores, o incluso ir firmadas o ser atribuidas a personas de cierta relevancia. Es importante enseñar a los más jóvenes a identificarlas. Para hacerlo, la mejor y más rápida opción es **acceder a Google, y teclear el titular de la noticia o información, siempre entre comillas.** Si al hacer esto, la noticia no aparece en ningún medio, podemos descartarla. Del mismo modo podemos buscar también al supuesto firmante.

Por norma general se recomienda desconfiar y verificar especialmente:

- Mensajes que nos llegan con errores de expresión, incongruencias de género o número, y faltas de ortografía.
- Mensajes que pretenden llamar nuestra atención generándonos sentimientos o emociones de algún tipo. Las noticias falsas intentan que las difundamos, y lo suelen hacer apelando a nuestra faceta más emocional.
- Mensajes con una clara tendencia ideológica que pretenden generar indignación.

3. ¿Con cuántas horas de uso de internet al día se puede considerar que tengo una adicción?

No podemos valorar un posible trastorno adictivo por el número de horas que le dedicamos a una actividad. El factor tiempo no es el más importante. De hecho, hay niños que dedican más tiempo que otros a una actividad, como los videojuegos, sin desarrollar ningún trastorno. Y amigos suyos que juegan menos horas pueden estar desarrollando una adicción.

Para valorar un posible problema de este tipo en un niño o adolescente, hemos de tener en cuenta entre ocho y diez criterios de valoración distintos. Por ejemplo, un criterio que valoramos es la presencia o no de un síndrome de abstinencia. Es decir ¿cada vez que le pedimos que deje la actividad se enfada, desarrolla ira, da un portazo o un puñetazo en la mesa? Ese sufrimiento que se produce al tener que dejarlo es muy significativo. Deberemos valorar también el desarrollo de tolerancia, como sucede con las sustancias. Es decir

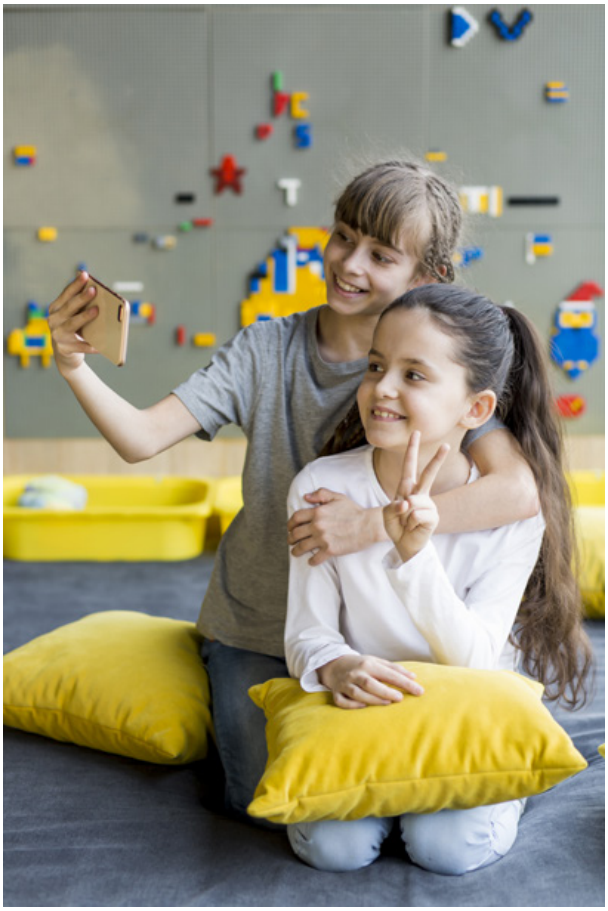
¿lo que hacía ya no le satisface y siempre quiere un poco más? Debemos observar si se produce un uso compulsivo: ¿siempre que tiene un momento libre lo primero que hace es acudir a esa herramienta? Y así hasta diez criterios.

Si queremos centrarnos en una única cuestión, la pregunta que debemos hacernos es: **¿el uso de esa herramienta está condicionando el resto de facetas de su vida?** Si por esa herramienta ha suprimido el resto de formas de ocio con las que disfrutaba, si dedica cada vez menos tiempo a sus obligaciones, si entra en conflicto constantemente con sus padres, si cuando llega la hora de acostarse se va con la tableta a la cama y no duerme lo necesario… es cuando podemos concluir que hay un problema. Lo consideraremos una adicción si la herramienta está modificando y condicionando negativamente su vida.

4. Si utilizo un nombre inventado cuando me creo una cuenta en internet, ¿puedo estar cometiendo un delito?

Debemos tener clara la diferencia entre inventarse un nombre y utilizar el nombre de otra persona. El hecho de **inventarse un nombre para moverse por internet NO es un delito.** Es más, cuando los menores de edad utilizan servicios como redes sociales o videojuegos, se recomienda precisamente que inventen un nick o apodo. Por ejemplo: araña negra. No aporta información personal y permite mantener nuestra privacidad. Ahora bien, algunos servicios de internet exigen a sus usuarios utilizar sus nombres, y no aceptan identidades inventadas. Contravenir las normas de esa herramienta puede conllevar la suspensión de la cuenta. Muy distinto es utilizar una identidad que se corresponde con la de otra persona, con el objetivo de hacernos pasar por ella, tal y como se explica en otra pregunta.

5. ¿Puedo publicar una foto de mi cumpleaños con mis amigos si tengo su permiso?



La foto del rostro es un dato personal, como puede serlo el número de teléfono o la dirección física de una persona. Por lo tanto, para publicar fotografías o datos personales de terceros necesitamos su consentimiento previo. En el caso de los menores de edad, existe una frontera muy importante en los 14 años. **Para publicar fotografías de un menor, con edad inferior a 14 años, es necesaria la autorización de los padres,** siempre y cuando ambos tengan la patria potestad.

A partir de los 14 años el adolescente puede autorizar directamente la publicación de su imagen, pero no antes. Es decir, los niños que no llegan a esa edad no pueden consentir la difusión de su imagen ni de otros datos personales, por lo que será necesaria la autorización de los padres. Esta obligación también les incumbe a ellos, así que para publicar fotos o vídeos en los que se pueda ver la cara de sus amigos/as deberán tener permiso de los padres de estos. Debe ser así siempre que el menor sea reconocible. Es decir, si aparece con el rostro tapado, de espaldas, o a una distancia tal que no es reconocible, no será necesaria entonces dicha autorización.

Difundir la imagen de niños sin la autorización de sus padres o tutores legales conlleva sanciones económicas.

Cabe señalar que esto no es así en todos los países. El Reglamento General de Protección de Datos (RGPD), aprobado en Europa en 2016, señala que el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años, pero, permite a los distintos Estados miembros modificar esta edad. España lo hizo y la rebajó a los 14 años.

6. Cuando hago una búsqueda en Google ¿me puedo fiar de los resultados?

En realidad, para esta cuestión da lo mismo hacer la búsqueda en Google que en cualquier otro buscador, en cuanto a que los buscadores solo organizan una parte de la información que circula por internet. Dichos buscadores clasifican los resultados de las búsquedas atendiendo a criterios de posicionamiento. Estos criterios tienen que ver con la utilización de palabras clave, el tipo de enlaces incluidos, la velocidad de carga y otros muchos, pero **pueden enlazar a sitios con información no contrastada, caducada o tergiversada.** Del mismo modo, sitios que cumplen muchos criterios de posicionamiento pueden aparecer más arriba que sitios más interesantes y serios que no los cumplen.

Para los niños, además, no siempre resulta fácil diferenciar lo que es publicidad de lo que no. Los primeros resultados que suelen aparecer son anuncios pagados, sencillamente. Según el informe Niños y Padres: Medios y Actitudes, publicado por la entidad británica OFCOM: casi el 70% de los niños de 12 a 15 años de edad es incapaz de distinguir los resultados ofrecidos por el buscador de los anuncios pagados que aparecen en los resultados de las búsquedas.

Es necesario trabajar con niños y adolescentes sobre lo que conocemos como técnicas de curación de contenidos, que les permiten encontrar los mejores resultados de entre los millones de opciones que ofrecen los buscadores. Del mismo modo, deben aprender técnicas de verificación de contenidos. En no pocas ocasiones copian y pegan en sus trabajos información no contrastada, o que proviene de sitios en los que aparecen y desaparecen las famosas fake news o noticas falsas.

7. Cuando me desinstalo una aplicación, ¿pueden seguir accediendo a los contenidos de mi móvil o tableta?

Instalar una aplicación sin leer los términos y condiciones de uso es lo más habitual, no solo entre niños y adolescentes, sino también entre adultos. Dicha

instalación implica una serie de permisos y autorizaciones que es muy importante leer. En muchas ocasiones se otorga permiso para que la app acceda a nuestra galería de fotos, a nuestra agenda de contactos, a nuestra ubicación y a toda una serie de datos muy sensibles.

Muchos menores de edad instalan además estas apps en los móviles y tabletas que utilizan sus padres, de tal forma que están permitiendo el acceso a información personal o incluso laboral de sus progenitores.

Cuando desinstalamos una aplicación ya no puede acceder a los contenidos de nuestro dispositivo. Ahora bien, lo que vaya a suceder con los datos que ya hemos facilitado, y que además pueden haber sido cedidos a terceros, no podremos saberlo realmente. En primer lugar es recomendable eliminar todos los datos, fotos y demás archivos que podamos tener en dicha aplicación. Después de esto hay que proceder a la desinstalación. Si se trata de una red social o similar, deberemos además **dar de baja o cancelar la cuenta,** ya que si solo borramos la aplicación de nuestros dispositivos, esta seguirá existiendo.

Como siempre: lo mejor es leer antes de instalar.

8. ¿Puedo ponerme de foto de perfil, la foto de un famoso que he encontrado en internet?

Con frecuencia niños y adolescentes publican fotografías de sus personajes favoritos de películas o de series de televisión, deportistas, cantantes y todo tipo de personas que comúnmente conocemos como personajes públicos. No obstante, el hecho de que tengan una repercusión mediática no nos autoriza a utilizar su imagen. Es cierto que dicha imagen no suele ser publicada por los menores de edad para hacerse pasar por los famosos, o conseguir visitas o seguidores, pero el hecho de que no se trate de usurpaciones de identidad no les exime de responsabilidad.

La imagen de cada persona es considerada un dato personal, y para hacerla pública en internet necesitaríamos el consentimiento de la persona que aparece en la fotografía. Existen excepciones, como aquellas imágenes obtenidas en eventos de interés informativo, en las que prima el derecho a la información sobre el derecho a la propia imagen. Cuando no está claro cuál de los dos derechos prima, será un juez el que tendrá que determinarlo. No obstante, ese no suele ser el caso, y los menores de edad que utilizan esas imágenes lo hacen como seguidores o fans del personaje público. En estas circunstancias es difícil que se llegue a producir una denuncia, a no ser que se esté causando un perjuicio al personaje; pero, no estamos hablando solo del derecho a la imagen, sino también de los derechos de autor. La fotografía que está publicando el menor seguramente ha sido obtenida por un profesional, y tal vez incluso comprada por un medio de comunicación online que habrá adquirido los derechos. Ponernos de foto de perfil la foto de un famoso puede acarrear **problemas tanto con el personaje público como con el autor de la fotografía.**

9. ¿Alguien me podría ver a través de la cámara del ordenador o de la tableta?

En efecto, **la posibilidad de que alguien pueda activar por remoto nuestra cámara, desde otro terminal, realmente existe,** siempre que se trate de una herramienta con cámara incorporada y conexión a internet. Ahora bien, para que esto suceda, es necesario que nos instalemos antes un programa malicioso que permita al ciberdelincuente activar nuestra cámara. Estos programas de tipo spyware se instalan sin que nos demos cuenta al descargarnos archivos con virus.

Para evitar la descarga de malware de este tipo es necesario tener mucho cuidado con los sitios que visitamos en internet, y con los archivos que abrimos. También es importante tener instalado un antivirus en nuestros dispositivos para identificar e impedir la descarga de programas maliciosos. Muchas personas, además, llevan tapada la cámara de sus dispositivos con una pegatina o un sistema de ventana de plástico, para que si se activa la cámara sin su conocimiento no pueda grabar ninguna imagen.

10. ¿Algunos videojuegos pueden ser más adictivos que otros?

Algunos videojuegos responden a **una serie de características que aumentan considerablemente su potencial adictivo,** y son sin duda más problemáticos. Por ejemplo, aquellos que disponen de una faceta social, es decir, que permiten a los niños y adolescentes relacionarse con otros, resultan mucho más atractivos y es más difícil dejarlos. Lo mismo sucede con aquellos que nos permiten marcarnos objetivos numéricos y sin un límite que resulte posible alcanzar. También aquellos que nos facilitan escoger y crear nuestra propia identidad, y de forma especial aquellos que ofrecen una relación y frecuencia alta entre estímulos y respuestas. La presencia de recompensas impredecibles, la posibilidad de progresar, y otras técnicas, hacen que resulte muy costoso prescindir de una herramienta.

El hecho de utilizar un videojuego con un potencial adictivo elevado, no implica necesariamente que el usuario vaya a desarrollar un trastorno adictivo. Las características de la persona resultan muy importantes. Una puede desarrollar el problema mientras otra en absoluto.

11. ¿Insultar o amenazar a otras personas utilizando emoticonos es como hacerlo con palabras?

Algunos niños y adolescentes tienden a pensar que las acciones que llevan a cabo cuando se relacionan en los entornos digitales no revisten demasiada importancia, o al menos no tanta como cuando se relacionan cara a cara. Esto no es así en absoluto. **Desde el punto de vista psicológico por supuesto que resulta igual de dañino insultar o amenazar a otras personas, pero también puede serlo desde el punto de vista jurídico.**

El significado de los emoticonos o emojis depende del contexto en el que se utilicen y la finalidad que tengan en cada con-versación. De hecho, son interpretados en nuestro cerebro por las mismas zonas que utilizamos para reconocer las expresiones de las caras de personas con las que hablamos de forma presencial. Su presencia en un mensaje de texto o en un correo electrónico puede aclarar el significado del mismo, reforzarlo o incluso potenciarlo.

Del mismo modo, enviar emojis se considera una comunicación a efectos legales. El primer caso del que tenemos conocimiento en relación a esta cuestión se produjo en 2015, cuando un joven de Nueva York colgó un mensaje en Facebook con el pictograma de un policía y tres pistolas consecutivas. Esta frase en imágenes se consideró una clara amenaza de muerte. De hecho, Apple decidió eliminar este emoji y sustituirlo por una pistola de agua. En España, en 2018, la Sección Primera de la Audiencia Provincial de Alicante condenó a nueve meses de prisión, por un delito de quebrantamiento de condena, a un hombre que envió dos emoticonos a su expareja, cuando una condena anterior le había prohibido comunicarse con ella. Los emoticonos también son algo serio.

12. ¿Cualquiera puede ver mi foto de perfil cuando utilizo Whatsapp?

Muchos adolescentes tienen un perfil de Whatsapp público, que **permite a cualquier persona hacer un seguimiento de las fotografías que van su-**

biendo a dicho perfil, así como de su estado. Cuando incluimos un número de teléfono en nuestra agenda, podemos acceder a la fotografía que utiliza ese usuario para mostrarse a los demás, o podemos no verla. Si vemos esa foto y su estado es cuando decimos que su perfil es público.

Esto es poco aconsejable, no solo para los adolescentes, sino también para los adultos. Si somos de esas personas que tienen la misma fotografía desde hace meses o años, y se trata de la foto de un paisaje o una frase de Einstein, no tenemos que preocuparnos. Pero si, por el contrario, somos de las personas que cambian su perfil con frecuencia, y ponen imágenes de sus familiares, actividades de ocio, en el trabajo o en el colegio, o que permitan determinar creencias religiosas o políticas, tal vez no estamos protegiendo correctamente nuestra privacidad.

Para configurar bien la privacidad en whatsapp debemos:

- Acceder a nuestra aplicación de Whatsapp y tocar sobre la ruedecita de CONFIGURACIÓN. Entrar después en CUENTA y, a continuación, en PRIVACIDAD.
- Ahí debemos tener seleccionadas las opciones de SOLO MIS CONTACTOS.

Si por el contrario tenemos seleccionada la palabra TODOS, cualquier persona que conozca y grabe nuestro número, o que lo incluya en su agenda por error, estará viendo nuestro perfil.

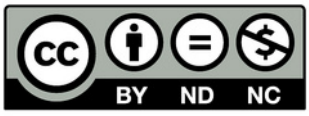
13. ¿Qué fotos de las que me encuentro en internet puedo utilizar libremente?

El uso de los contenidos que encontramos en internet debe ajustarse a las leyes que regulan los derechos de autor y de propiedad intelectual. Algunos contenidos son de libre uso, otros requieren cumplir una serie de requisitos, y otros implican la adquisición de derechos y licencias que tienen un pequeño coste económico.

Si queremos que nuestros hijos utilicen con tranquilidad y de forma gratuita fotografías para sus trabajos de clase, sus blogs o sus perfiles en redes socia-

les, **es recomendable utilizar imágenes copyleft con derechos cedidos,** como las identificadas por la organización sin ánimo de lucro creative commons. Estas imágenes, vídeos, textos y demás contenidos son identificadas mediante la utilización de una serie de símbolos que especifican las condiciones bajo las que pueden utilizarse. Cuando aparecen estos símbolos podemos utilizar dichas imágenes, pero cuando no aparecen en la web en la que nos encontramos debemos entender que no pueden utilizarse.

Símbolos que identifican los contenidos creative commons:



BY: Debemos identificar con su nombre al autor de la obra.

ND: No podemos alterar la obra.

NC: No podemos utilizar la obra con fines comerciales.

Buscador de contenidos CC:
https://ccsearch.creativecommons.org/

14. ¿Mis padres pueden grabarme en una actuación del colegio?

Cuando las fotografías o filmaciones son obtenidas por familiares de los alumnos, se trata de personas físicas en actividades consideradas personales o domésticas, por lo que no sería de aplicación el Reglamento General de Protección de datos. Es decir, los padres **pueden obtener dichas imágenes de sus hijos durante las actuaciones en festivales escolares.** No obstante, deberán ser de uso personal y de ninguna manera podrán ser publicadas en redes sociales o en otros entornos digitales. Para hacer esto deberán contar con la autorización de los padres de los demás niños/as que aparezcan en las imágenes. Es recomendable recordar esto último a las familias de forma previa a las actuaciones.

Esto será así siempre y cuando no exista una norma en contra. Es decir, los colegios, al amparo de la Ley Orgánica de Educación, podrán aprobar y ejecutar normas de organización en el centro que desautoricen estas prácticas.

15. ¿Puedo descargarme sin querer un virus en mi móvil o en mi tableta?

Muchos alumnos no saben que **los teléfonos inteligentes y las tabletas también pueden sufrir ataques de virus informáticos.** Por otro lado, en la mayoría de los casos tienden a pensar que estos programas pueden dañar nuestros aparatos, quitarles capacidad, memoria, velocidad o simplemente reducir la vida de la batería. Sin embargo, los virus que existen en la actualidad no solo pueden atacar cualquier aparato conectado a internet, sino que además son capaces de robar toda la información que se encuentra en su interior, ubicar nuestros domicilios, grabarnos y filmarnos.

Algunos programas de este tipo han sido creados para permitir a otras personas manejar nuestros dispositivos a distancia, suscribirnos a servicios de pago, o realizar acciones delictivas desde los mismos. Además, pueden llegar a hacer esto sin que notemos nada extraño en el funcionamiento del terminal.

La principal recomendación es muy clara, al margen de evitar los sitios en los que suelen encontrarse este tipo de programas maliciosos: deben tener instalados programas antivirus en los terminales que utilizan. Si bien son mucho más necesarios en unos aparatos que en otros, siempre deben llevarlos instalados y operativos. Es importante, así mismo, actualizar el antivirus constantemente. Si no lo actualizan, no podrán protegerse de los virus nuevos que comienzan a circular cada día. Del mismo modo deben actualizar siempre el sistema operativo, y programas y aplicaciones que tengan instaladas. Muchas actualizaciones se hacen precisamente para cubrir agujeros de seguridad. También es posible configurar las actualizaciones para que realicen de forma automática.

16. ¿Cómo puede llegar a infectarse con un virus mi móvil, tableta u ordenador?

Los virus se propagan de forma muy rápida, y en ocasiones es suficiente con abrir una foto que hemos recibido o pinchar en el enlace equivocado. La mayor parte de las infecciones se producen en las siguientes situaciones:

- Abriendo un correo de alguien desconocido, con un archivo adjunto o una simple fotografía. Si el dispositivo de algún amigo/a ha sido infectado, también podemos recibirlo en un correo con su remitente.
- Un mensaje, o incluso un whatsapp, con un enlace a una página web con código malicioso.
- La descarga de una actualización o de un archivo desde una página no oficial.
- La descarga de una aplicación móvil desde una web no oficial.
- La descarga de una aplicación desde una tienda oficial, pero que aún no ha sido verificada (más probable en Google Play).
- La descarga de archivos de música, películas o de otro tipo, a través de programas de p2p (peer to peer), como el Emule o el Ares.
- La descarga de archivos en la red profunda, o Deepweb, la parte de internet en la que se encuentra el mayor volumen de contenidos, y que no es accesible para buscadores como Google.

Al margen de las herramientas que nos ofrece la propia tecnología, debemos educar a nuestros hijos para que sepan cómo realizar un uso adecuado del terminal, y cuáles son las situaciones de riesgo que suelen facilitar la descarga de este tipo de virus informáticos.

17. ¿Para qué quieren las redes sociales mis datos personales?

Esta es una de las preguntas que surgen con más frecuencia cuando se trabaja el tema de las redes sociales en el aula, especialmente entre los alumnos de más edad. Y normalmente surge tras descubrir que al crearse un perfil han aceptado esta y otras muchas condiciones.

Los datos personales del usurario son utilizados para obtener beneficios económicos, normalmente a través de la publicidad. Cuantos más datos personales maneja una red social más puede personalizar sus anuncios y, por supuesto, más capacidad tiene para influir sobre las decisiones del usuario. Según los expertos, gracias a nuestros datos personales **se obtienen unos beneficios que oscilan entre los 200 y los 2.000 euros por usuario**[1]

Al margen del interés económico de la redes sociales, se encuentran los intereses de otras muchas empresas que obtienen datos de los usuarios de tales redes o a partir de la descarga de las cookies. Esta información se puede utilizar para influir sobre los usuarios no solo como consumidores, sino incluso como futuros votantes. El caso más conocido es el de la empresa Cambridge Analytica, que obtuvo datos de millones de usuarios de Faceboock para influir sobre su voto en las elecciones de Estados Unidos.

Los usuarios más jóvenes deben saber también que existen empresas de data brokers, cuyo trabajo consiste en recopilar datos personales de todos los entornos posibles y cruzarlos entre sí, para venderlos y obtener importantes beneficios económicos.

18. ¿Es verdad que no se sabe dónde terminan mis vídeos de TikTok?

Esta pregunta es de fácil respuesta, ya que no podemos saber el uso final que se le da a los vídeos y datos obtenidos de los mismos. Por esta razón, es bueno enumerar una serie de informaciones que confirman una realidad: **algunas**

1. El Mundo. 5 de abril de 2021. «¿Cuánto valen sus datos?».

entidades no hacen solo lo que dicen que van a hacer, sino también lo que no dicen.

TikTok acaba de ser multada con 750.000€ en Holanda por incumplimiento de la normativa de protección de datos, lo cual ha afectado a un gran número de menores de edad. Pero esta no es la primera vez. En abril de 2021, se presentó en Reino Unido una demanda acusando a TikTok y a su empresa matriz china ByteDance, de recopilar ilegalmente datos personales de millones de niños en el Reino Unido y Europa. Anteriormente, cuando TikTok se conocía como Musical.ly, ya se le impuso una sanción de 5,7 millones de dólares por las mismas razones en Estados Unidos.

También en 2021, la Organización Europea de Consumidores (BEUC), que aglutina a 15 países europeos, inició acciones contra TikTok ante la Comisión Europea. En España, la OCU se ha dirigido también a la Agencia Española de Protección de Datos (AEPD), y al Ministerio de Consumo, presentando una conciliación judicial ante la Comisión Nacional de los Mercados y la Competencia (CNMC). La investigación realizada por BEUC concluye que TikTok comete múltiples violaciones de los derechos del consumidor en la UE, y no protege a los niños de la publicidad oculta y el contenido inapropiado, entre otras cuestiones[2].

19. ¿Algo que cuelgo en una red social, puede aparecer dentro de años y afectar a mi futuro?

Entre el alumnado de más edad esta es una cuestión que preocupa cada vez más, y con razón. Los datos personales que vamos publicando o compartiendo en internet, más los que comparten nuestros conocidos, más

2 https://www.beuc.eu/publications/beuc-x-2021-012_tiktok_without_filters.pdf

los que se obtienen de nuestra actividad en línea, conforman lo que denominamos habitualmente reputación digital.

Nuestra reputación digital puede condicionar las decisiones de personas que pueden incidir sobre nuestro futuro. Si un alumno/a piensa estudiar algún curso en otro país, pedir una beca, ir a una universidad privada o, sencillamente, acceder a un puesto de trabajo en el futuro, debe saber que es muy probable que **las personas que tomarán la decisión de entrevistarlo o no, consultarán primero la información disponible en internet. Y esta información puede ser determinante.** Estos datos lo confirman[3]:

- El 86% de las empresas reconoce que revisa los perfiles de los candidatos en las redes sociales cuando inician un proceso de selección de trabajo.
- El 70% de los responsables de los departamentos de Recursos Humanos considera clave la información encontrada en las redes sociales.
- El 36% de las empresas ha desestimado la candidatura de algún aspirante a un puesto de trabajo por la imagen que proyecta en las redes sociales.

20. ¿Cómo pueden suplantar mi identidad en una red social?

Las suplantaciones de identidad son cada día más frecuentes, y en función del objetivo con el que se lleven a cabo pueden dar lugar a multitud de problemas. Alguien que adopta nuestra identidad para estafar o cometer delitos en internet, para amenazar o menospreciar a otras personas, y todo ello en nuestro nombre, puede generarnos incluso problemas legales.

Estas suplantaciones de identidad suelen llevarse a cabo de dos maneras. Por un lado **es posible que alguien utilice la propia cuenta del adolescente para hacerse pasar por él.** Esto sucede cuando esa persona consigue su contraseña y accede sin problemas. En estos casos suele tratarse de algún conocido al que se la ha dado en alguna ocasión, o tal vez le han visto teclearla. También puede que resulte demasiado sencilla, o que sea la misma que utiliza en otras cuentas. Si alguien le ve poner su contraseña en el correo elec-

3 Datos del Informe Redes Sociales y Mercado de Trabajo de Infoempleo y Adecco, y de la encuesta realizada por InfoJobs.

trónico, y es la misma que usa en una red social, podrá acceder a su cuenta sin más complicaciones. En la mayoría de estas ocasiones se tratará de una broma, pero si no es así y le cambian la contraseña para que ya no pueda entrar, entonces debe comunicarlo a la red social y poner una denuncia.

La otra forma, que nos preocupa más, es que hayan **creado un perfil simulando ser el del nuestro hijo/a.** Para ello pueden clonar su perfil, e incluso utilizar las mismas fotografías que hay en el perfil original. Nuestros hijos han de saber que esto es grave y que deben decírnoslo inmediatamente si llega a producirse. Será necesario poner una denuncia, y comunicarlo a la Agencia Española de Protección de Datos, además de notificarlo directamente a la red social para que eliminen ese perfil.

21. ¿Qué puede llegar a hacer alguien que suplanta mi identidad en internet?

Los daños que pueda causar quien lo hace, dependerán de las intenciones e imaginación que pueda tener, pero identificamos cuatro grupos de problemas:

- PROBLEMAS DE REPUTACIÓN DIGITAL. Esa persona puede utilizar nuestro perfil para decir barbaridades, para apoyar a grupos radicales de cualquier tema, colgar imágenes o vídeos para que los demás piensen que nosotros pensamos de esa manera, etc. Eso puede suponer un problema importante para nuestra imagen si lo hace públicamente.
- PROBLEMAS DE CONVIVENCIA. Es posible utilizar ese perfil para generarnos conflictos con las personas con las que nos relacionamos de forma habitual. Si conoce a nuestras amista-des, compañeros del colegio, profesores o vecinos, puede dedicarse a insultarlos en nuestro nombre, enviarles

imágenes desagradables, etc. Si creen que ese perfil es nuestro, tendremos que dar muchas explicaciones para que todo el mundo nos crea.

- PROBLEMAS DE SEGURIDAD. Hay que tener muy mala idea, pero podría utilizar ese perfil falso para amenazar o provocar a personas peligrosas. Podría insultar a un grupo problemático de otro centro y citarlos a la salida de nuestro colegio… Podría también contratar en nuestro nombre servicios por los que después no pagaría y generarnos una deuda, etc.
- PROBLEMAS LEGALES. También es posible utilizar esa cuenta falsa para difundir mensajes ilegales o contenidos que son delictivos. También existe la posibilidad de que la utilizara para cometer estafas, engañar a otras personas utilizando nuestra identidad o incluso participar en ataques informáticos a otros usuarios desde nuestro supuesto perfil.

22. ¿Por qué no debo dejar que me sigan cuentas temáticas?

Los usuarios más jóvenes siguen habitualmente cuentas de redes sociales temáticas o genéricas, es decir, perfiles cuyo contenido está centrado en un tema determinado. Este tema puede incluir desde contenidos relativos a grupos musicales o series de televisión, hasta deportes, manualidades, ropa o cuentas de fans de famosos. Algunas de estas cuentas pueden ser oficiales, pero hay miles de cuentas cuyos creadores no se han identificado de ninguna manera. Cualquiera puede crear un perfil y colgar sus outfit con prendas de distintas marcas de ropa, o montarse un club de seguidores de lo que sea.

Seguir este tipo de perfiles no conlleva ningún riesgo en sí, más allá de identificarnos como simpatizantes o seguidores de algo en concreto. Esta información podrá ser utilizada después con fines comerciales entre otros, evidentemente.

El problema surge cuando el menor de edad recibe después una solicitud de seguimiento de ese perfil, es decir, que ahora es el creador de dicho perfil el que quiere ver los contenidos que ha subido nuestro hijo/a. **Si son demasiado confiados, o piensan que por ser un perfil sobre o un tema y con**

muchos seguidores, no pasa nada, pueden estar abriéndole la puerta a alguien indeseable. Desconocemos totalmente las motivaciones de la persona o personas que están detrás.

Los perfiles que siguen dicen mucho sobre quiénes son, y deben cuidarlos cara a su reputación digital. Pero algunas de estas prácticas pueden afectar también a su seguridad. Su perfil personal debe ser siempre privado, y deben aceptar como amigos o seguidores solo a personas que conozcan realmente.

23. ¿Qué debo hacer si algún compañero/a me acosa en internet?

Denominamos ciberacoso o ciberbullying a toda agresión psicológica, sostenida y repetida en el tiempo, perpetrada por uno o varios miembros del alumnado contra otro, utilizando para ello las tecnologías de la información y la comunicación –TIC-. El protocolo básico a seguir es el siguiente:

1. NO RESPONDER A LAS PROVOCACIONES. En no pocas ocasiones, el compañero/a que acosa desiste si ve que no hay reacción por parte de quien lo sufre.
2. PEDIRLE QUE PARE. Si no cesa en su actitud, hay que pedirle que pare. Esto es así para dejar claro y por escrito que NO estamos interpretando la situación como “una broma”, y que nos está causando daño.
3. NO REACCIONAR NUNCA DE LA MISMA MANERA. Ante insultos y amenazas es importante no replicar la misma conducta.
4. BLOQUEAR. Muchas herramientas, sistemas de mensajería, redes so-

ciales y hasta videojuegos, permiten bloquear o silenciar a quien nos molesta.

5. DENUNCIAR EN EL SITIO. Está muy generalizada la presencia de botones de “denuncia” o “reporte” de conductas inapropiadas. Hay que utilizarlos.
6. HABLAR CON SUS PADRES. Si la situación continúa es necesaria nuestra intervención como padres. Una de las siguientes opciones es comunicarlo al colegio.
7. RECOGER PRUEBAS. A lo largo de todo el proceso es importante no borrar nada e ir guardando las pruebas de todo cuanto va sucediendo: mensajes e imágenes recibidas.
8. INTERPONER UNA DENUNCIA. Es la última opción, pero en ocasiones no queda más remedio que denunciar los hechos en una comisaría de policía.

24. Si un compañero/a del colegio me acosa en internet ¿puedo comunicarlo al colegio?

El ciberbullying suele estar protagonizado por compañeros/as del mismo centro. **Al comunicarlo se facilita la intervención de la comunidad educativa.** Si no se tiene constancia de los hechos no se puede llevar a cabo ninguna acción, por lo que llegado el caso es aconsejable trasladarlo. No obstante, esto es algo que deben decidir los padres del afectado, y una vez que los primeros pasos del protocolo anterior no han dado resultado.

En el caso de que la situación de acoso esté protagonizada por alguien que no se identifica, y solo tengamos sospechas, o cuando parece probable que se trate de alguien externo al centro educativo, la comunidad educativa no podrá intervenir. En estos casos se recomienda acudir directamente a la opción de la denuncia en una comisaría de la policía y, a ser posible, en las unidades especializadas en este tipo de supuestos.

Hemos de tener en cuenta que si los menores que acosan tienen menos de 14 años, no tienen entonces responsabilidad penal y, por lo tanto, no se les podrá imputar ningún delito. No obstante, aunque en estos casos no concurra responsabilidad penal, sí existirá una responsabilidad civil por los daños y per-

juicios ocasionados de la que responderán los representantes legales del menor acosador. (Artículo 1903 del Código Civil) Si los menores que acosan tienen entre 14 y 17 años será de aplicación la Ley Orgánica 5/2000, de 12 de enero, reguladora de la Responsabilidad Penal del Menor y, en consecuencia, desde la Fiscalía de Menores se incoará un expediente de reforma para investigar los hechos y se podrán adoptar medidas cautelares que pueden dar lugar al internamiento del menor en un centro de protección de menores, entre otras.

25. ¿Cómo distinguimos una broma del ciberacoso o ciberbullying?

Con frecuencia el alumno/a que lleva a cabo la acción se justifica señalando que todo se trataba de una broma. Y lo cierto es que en ocasiones puede comenzar de esta manera. Así pues, tal y como se recoge en el protocolo, el primer paso debe ser aclarar esta situación directamente, explicitando que el menor objeto de acoso no participa de tal broma.

La broma no depende de las veces que se repita, ni de su intensidad o publicidad. Depende de que sea aceptada como tal por quien la realiza y por quien la recibe. Es decir: **consideramos que algo es una broma cuando ambas partes se divierten.** En el momento en el que una de las dos partes no se divierte, no puede considerarse algo lúdico o bienintencionado.

Deberemos cerciorarnos siempre, por supuesto, de que no existen coacciones que lleven al menor objeto de la broma a aceptarla contra su voluntad, o justificarla por miedo a la reacción de los demás.

26. ¿Son realmente privadas las conversaciones que mantenemos de móvil a móvil por Whatsapp?

Las conversaciones que mantenemos por Whatsapp son privadas y están protegidas por un sistema de cifrado de móvil a móvil, lo que garantiza que solo pueden ser leídas por sus legítimos destinatarios.

No obstante, se recomienda utilizar el sistema de doble verificación para que Whatsapp confirme cada poco tiempo que somos quienes decimos ser y nadie está hablando por nosotros. Para hacerlo:

> WhatsApp > Ajustes/Configuración > Cuenta > Verificación en dos pasos > Activar

A partir de este momento, cada semana se nos vuelve a pedir el código. Si alguien nos robara el teléfono, solo podría usar nuestra cuenta de WhatsApp durante 7 días como máximo.

Al margen de las situaciones estándar, las conversaciones pueden ser desveladas por otros sistemas. Por ejemplo, cuando denunciamos un chat en la propia herramienta, se envían los cinco mensajes más recientes a Whatsapp para que la empresa pueda tomar una decisión sobre cómo proceder en ese caso. Y tampoco debemos olvidar que cualquier usuario con el que estemos hablando puede hacer capturas de pantalla de todo cuanto decimos y pasárselas a otras personas sin nuestro conocimiento.

La privacidad no depende solo de la herramienta, sino también de las personas que la están usando.

27. ¿Por qué es necesario tener cuidado con las aplicaciones que acceden a mi ubicación?

Las aplicaciones que nos solicitan permiso para acceder a nuestra ubicación o localización, **realmente están accediendo a un volumen ingente de información personal.** Si esa app tiene acceso a nuestra ubicación por las noches, lo que sabrá es dónde vivimos (tipo de vivienda, precio medio de las

viviendas… y hasta partido político que ha ganado las elecciones en esa calle). Si lo hace durante el día sabrá dónde estudiamos (tipo de colegio). Sabrá también qué tiendas frecuentamos, restaurantes, dónde pasamos los fines de semana, dónde veraneamos y cuándo, si hemos asistido a una manifestación o dónde estamos los domingos por la mañana. Deberíamos sopesarlo.

28. ¿Qué son las cookies en internet y para qué sirven?

Las cookies son ficheros de datos que las páginas web descargan a través de nuestros navegadores. Sirven para que **los sitios en los que entramos puedan identificar nuestro dispositivo y recordar todo lo que hemos visitado.**

Cuando aceptamos la descarga de las cookies, estas toman nota de los productos o temas que nos interesan, y le pasan esa información a otros sitios. Cuando visitamos esos otros sitios, ya saben qué es lo que nos atrae y nos lo ofrecen. Podemos decir que existen dos grandes tipos de cookies: las temporales y las permanentes:

- Temporales. Solo funcionan mientras estamos en la página que nos ha solicitado la descarga. Una vez que salimos de esa web, no se quedan en nuestro dispositivo.
- Permanentes. Se quedan instaladas en nuestro dispositivo para identificarnos cada vez que entramos.

Además, hay otros tipos de cookies. Algunas de las que más nos interesan son:

- Propias. Como su nombre indica pertenecen a esa web, y recogen datos para conocer con detalle todo lo que hacemos en la misma, las compras que hemos realizado, etc.
- De terceros. Pertenecen a otras empresas que han acordado con esa web la descarga de sus cookies. Es decir, cuando nos las descargamos esas empresas van a recopilar también toda la información sobre lo que hacemos.

En todos los casos es recomendable rechazarlas, aunque en algunos casos nos obligan a aceptar las propias.

29. Si es bueno eliminar las cookies ¿cómo se borran?

En efecto, es preferible eliminar las cookies que se hayan podido descargar después de cada sesión. Hacerlo aumenta nuestra seguridad y nuestra privacidad.

Si utilizas el navegador Chrome **en tu ordenador,** abre el menú de opciones, tocando en el botón de los tres puntos. Después:

Historial > Borrar datos de navegación

Si utilizas un móvil o tableta que funcione con Android, entonces debes hacer lo siguiente, en función de que tu navegador sea Chrome o Firefox:

Chrome para Android:

Abrir el menú de opciones, tocando en el botón de los tres puntos. Después:

Configuración > Privacidad > Borrar datos de navegación

Firefox para Android:

Abrir el menú de opciones, tocando en el botón de los tres puntos. Después:

Configuración > Limpiar datos privados > Cookies y sesiones activas

Si utilizas un móvil iPhone o un iPad:

Ajustes > Safari > Borrar historial y datos de sitios web

Para borrar las cookies y conservar el historial:

Ajustes > Safari > Avanzado > Datos de sitios web > Eliminar todos los datos

30. ¿Son peligrosas las direcciones acortadas y los códigos QR?

Cuando navegamos por una página web la dirección puede irse haciendo cada vez más larga, de tal forma que si la copiamos y pegamos en un documento puede llegar a ocupar varios renglones. Al enviársela a alguien puede romperse. En otras ocasiones lo que nos sucede es que queremos facilitar una dirección web -o URL- para que otras personas la copien, y si es muy larga se hace pesado hacerlo. Para evitar este tipo de situaciones existen los acortadores de direcciones. Lo que hacen es sustituir la dirección original por una mucho más corta, fácil de copiar y difundir. Es decir, en un principio es un servicio muy interesante.

El problema es que al ocultar la verdadera dirección a la que nos dirige, no podemos saber exactamente dónde vamos. Si resulta que dicho enlace acortado nos dirige a una web de contenido inapropiado o desagradable, o a una web que suplanta a otra oficial, o que contiene código malicioso provocando la descarga de virus, podemos tener un problema importante.

La recomendación es clara: no debemos pinchar en direcciones acortadas si no conocemos la fuente y nos ofrece confianza. **Debemos saber dónde nos lleva y quién nos la facilita. Exactamente lo mismo sucede con los códigos QR.**

Muchas direcciones acortadas comienzan por:

http://bit.ly | http://ow.ly | http://cut.ly

http://tinyurl | http://tiny.cc

31. ¿Qué es eso del spam? ¿Puede ser peligroso?

Denominamos spam al correo basura o no solicitado. Podemos recibir a diario mensajes, especialmente en el correo electrónico, en los que intentan vendernos algo u ofrecernos servicios de todo tipo: desde la venta de medicamentos con receta hasta pornografía. El problema del spam es que, al margen de que puede llevarnos a sitios desagradables o fraudulentos, puede también contener archivos maliciosos. Estos archivos suelen llegar en forma de vídeo, archivo comprimido, ejecutable, etc. Al pinchar en dicho archivo **se suele descargar un virus que puede desde causar un daño irreversible hasta robar todos nuestros datos y contraseñas.** En este caso forma parte de lo que denominamos fishing.

Muchos correos de spam son en realidad ataques de fishing que buscan, mediante diversos sistemas, obtener nuestra información personal o estafarnos. Es importante no abrirlos y eliminarlos, marcarlos como spam o denunciarlos.

32. ¿Qué es el fishing y la ingeniería social?

Podríamos definir el fishing como el **conjunto de técnicas que se desarrollan para lograr, mediante el engaño, datos sensibles de usuarios de internet:** desde sus números de tarjeta de crédito a sus claves de acceso a distintos servicios. Estos ataques son una verdadera amenaza para nuestra seguridad y la de nuestras familias, y están aumentando de forma exponencial.

Los ataques a personas son habitualmente más comunes y sencillos, y suelen llevarse a cabo de forma masiva. La inmensa mayoría de los ataques de fishing

tienen éxito gracias a errores humanos. Personas que abren un documento adjunto que no deberían haber abierto o que pinchan en un enlace que lleva a un sitio desconocido. El sistema más habitual que utilizan los ciberdelincuentes es el envío masivo de correos electrónicos con archivos adjuntos, o con enlaces a sitios supuestamente oficiales. De hecho, el 93% de los ciberataques comienzan con un simple correo. Otros ataques se producen a partir de mensajes por Whatsapp o privados en redes sociales. Un tercer sistema también utilizado para la distribución de virus es la creación de aplicaciones con el código malicioso ya incorporado.

Ingeniería social es la terminología que utilizamos al referirnos a la labor de investigación que se lleva a cabo para obtener información sobre una persona, con el objetivo de hacerla más accesible. Implica además el posterior desarrollo de técnicas y estrategias personalizadas, para lograr que dicha persona facilite sin quererlo el acceso a su terminal o a su información más personal. Conlleva por tanto una labor de investigación previa y un posterior engaño. La víctima puede incluso no ser consciente en ningún momento de la situación que se está desarrollando.[4]

33. ¿Cuándo decimos que una contraseña es realmente segura?

Consideramos que una contraseña es realmente segura **cuando no la conocen otras personas, y cuando no es fácil descubrirla.**

Para niños y adolescentes la primera cuestión es más impor-tante de lo que pudiera parecer, ya que en ocasiones se dicen las contraseñas unos a otros cuando van a prestarse el móvil o la tableta unos minutos. Es lógico que los padres conozcan nuestras contraseñas, pero no deben conocerlas también sus amistades.

En segundo lugar, para utilizar contraseñas seguras debemos tener en cuenta las siguientes premisas:

4 Ver Guía: CIBERSEGURIDAD FAMILIAR. Guillermo Cánovas

- Contraseñas alfanuméricas. Deben estar formadas por mezcla de letras y números, nunca solo letras.
- Mayúsculas y símbolos. Deberían contener también una mayúscula en algún sitio, no necesariamente al principio. Y si la herramienta lo permite también algún símbolo. Ej: @
- Distinta. No deben utilizar la misma contraseña para varias herramientas. Si alguien les ve introducirla en una, la probará en otras y podrá robarles las cuentas.
- Apuntada. Para no olvidarlas, deben escribirlas en un papel, que debe permanecer en su habitación.
- Renovarse. Deberían cambiarlas de vez en cuando, y no aceptar que el navegador las recuerde.

34. ¿Qué pasa si alguien coge mi móvil o mi tableta y hace algo ilegal?

Este es un riesgo real, del que nuestros hijos toman conciencia en cuanto trabajamos con ellos la cuestión de las responsabilidades. **Cada usuario es responsable de lo que entra y sale de su móvil, tableta u ordenador.**

Cuando prestamos nuestro dispositivo a alguien, o cuando no lo tenemos protegido con una buena contraseña, puede ser utilizado para llevar a cabo acciones ilegales. Una persona que utilizara el dispositivo de nuestros hijos con mala intención, podría crearse una cuenta de correo electrónico o en una red social para:

- Colgar o difundir contenidos ilegales.
- Manifestar opiniones y que parezca que es la forma de pensar de nuestro hijo/a.
- Generar problemas de convivencia o relación con personas conocidas, insultándolas o amenazándolas, por ejemplo.
- Solicitar u ofrecer servicios de todo tipo, legales o ilegales.
- Cometer estafas y engañar a otras personas.

En caso de producirse una denuncia seríamos los principales responsables. Toda esa responsabilidad recaería sobre nosotros. Si el dispositivo ha estado en manos de otra persona, tendríamos la dificultad de poderlo demostrar. Conclusión: **no se prestan ni el móvil ni la tableta, y si en alguna ocasión se hace, debemos permanecer junto a la persona que lo está utilizando.**

35. ¿Qué son contenidos ilegales en internet?

Las legislaciones de la mayoría de los países, y desde luego las europeas, consideran ilegales toda una serie de contenidos en internet. El hecho de reproducirlos, colgarlos o difundirlos supone la consecución de un delito y acarrea diferentes sanciones e incluso penas de prisión.

Consideramos contenidos ilegales aquellos cuya difusión, publicación o incluso tenencia están prohibidas. Son contenidos ilegales, por ejemplo:

- Las páginas, perfiles en redes sociales o foros en los que se promueva el racismo o la xenofobia.

- Los sitios en los que se incite al odio, o a cometer acciones contra otras personas por sus creencias, ideas, preferencias, tendencias sexuales, etc.
- Los sitios de apología del terrorismo, o en los que se enseñe a fabricar bombas caseras.
- Los sitios en los que se promueva el tráfico de drogas, se anuncie su venta, etc.
- Los sitios de pornografía infantil.

La difusión de otros contenidos puede ser ilegal también, por ser ilegal su difusión sin autorización. Así, es ilegal la difusión de contenidos protegidos por derechos de autor y propiedad intelectual, a no ser que se disponga de autorización. Del mismo modo, la difusión de datos personales sin la autorización de los dueños, o la difusión de datos de menores de 14 años sin la autorización de sus padres, son acciones ilegales.

36. ¿Qué sucede si hago algo ilegal en internet y tengo menos de 14 años?

En España **los menores de 14 años no tienen responsabilidad penal y no son imputables**. A partir de esa edad se aplica la Ley Orgánica 5/2000, de 12 de enero: Ley reguladora de la responsabilidad penal de los menores, que exige responsabilidades a las personas mayores de 14 años y menores de 18 por la comisión de hechos tipificados como delitos o faltas en el Código Penal o las leyes penales especiales. Para los mayores de 14 años de edad, se prevén todo tipo de medidas penales, que pueden ir desde el internamiento en régimen cerrado, hasta prestaciones en beneficio de la comunidad o la realización de tareas socio-educativas.

No obstante, el hecho de que los menores de 14 años no sean imputables, no quiere decir que sus acciones no tengan consecuencias. El artículo 61.3 de la LORPM dice: ”Cuando el responsable de los hechos cometidos sea un menor de dieciocho años, responderán solidariamente con él de los daños y perjuicios causados sus padres, tutores, acogedores y guarda-dores legales o de

hecho, por este orden." En consecuencia, **los padres de los menores deberán responder solidariamente de los actos cometidos por sus hijos.**

37. ¿Por qué es peligroso descargarse contenidos piratas?

Los ciberdelincuentes que desarrollan y difunden virus, y programas con código malicioso de todo tipo, normalmente pretenden infectar al mayor número posible de dispositivos. Suelen crear espacios llamativos, con falsos regalos, difundir millones de correos electrónicos con archivos infectados o enlaces a sitios fraudulentos, y mecanismos similares. Y uno de esos sistemas consiste precisamente en colgar archivos infectados en sitios donde la afluencia de internautas es numerosa. **Archivos alojados en sitios de contenidos piratas contienen con frecuencia virus de todo tipo.** Así mismo, quienes se los descargan no tienen a quien dirigirse después para hacer una reclamación o denuncia.

Por otro lado, debemos recordar que los contenidos piratas generan pérdidas muy importantes, y no solo a los autores y creadores, sino a todas las personas cuyos trabajos dependen de la industria editorial, el cine, los videojuegos y otras muchas relacionadas. Además, los piratas se benefician del trabajo de otros sin aportar nada y no pagan impuestos. Se trata además de algo ilegal, y no es lo que queremos que aprendan niños y adolescentes.

38. ¿Qué es el derecho al olvido y cómo puedo utilizarlo?

Desde 2014 el Tribunal de Justicia de la Unión Europea impone a los buscadores de internet el respeto a las normas de protección de datos de la Unión Europea. Esto quiere decir que, cuando se lo solicitamos, **tienen la obligación de eliminar los resultados de una búsqueda en internet en la que aparezcan nuestros datos personales o información no autorizada.**

Si nos encontramos con una página en la que se están publicando nuestros datos personales, o contenidos que nos causen un perjuicio como calumnias, injurias, fotografías nuestras colgadas sin consentimiento… podemos dirigirnos

a Google, Yahoo y demás buscadores, para solicitar la retirada de los enlaces a ese sitio. Es decir, cuando alguien nos busque en internet no aparecerán dichos enlaces. Hay que recordar que es el buscador el que valora y decide si procede eliminarlos.

Al margen, podemos emprender todas las acciones legales que creamos oportunas contra quien está publicando ese tipo de contenidos.

Para solicitar la retirada de los enlaces, podemos dirigirnos a:

Formulario en Google:
http://bit.ly/1oAsezu

Formulario en Bing:
https://binged.it/3sEnk8C

Formulario en Yahoo:
https://bit.ly/39vYjor

39. ¿Cómo puedo guardar y extraer del móvil una conversación de Whatsapp?

En ocasiones puede interesarnos salvar una conversación de Whatsapp, y además extraerla del propio smartphone. Esta es una acción recomendada para situaciones de ciberacoso, por ejemplo, para conservar los contenidos antes de que puedan borrarse. Al mismo tiempo que guardamos la conversación podemos salvar también las imágenes que hayan podido enviarnos durante el transcurso de la conversación. No debemos olvidar que el móvil puede perderse, romperse o puede ser robado, con lo que perderíamos aquella información que no hubiera sido almacenada en otro dispositivo.

Para salvar una conversación en Whatsapp, **hacemos clic**

sobre el nombre de la persona con la que estamos hablando, o sobre el nombre del grupo de Whatsapp en el que se está produciendo la situación. Se abrirá un menú. **Abajo tenemos la opción de EXPORTAR.** Al clicar se creará automáticamente un archivo de texto con toda la conversación. Podemos guardar en la misma carpeta las imágenes, fotos o memes recibidos. Tendremos, además, la opción de enviar toda la información salvada a nuestro correo electrónico o subirla a la nube.

40. ¿Es verdad que los aparatos, incluso los televisores, pueden escucharme?

Cuando nos descargamos una aplicación deberíamos leer los permisos que estamos concediendo. Hemos de comprobar si nos están solicitando acceso a nuestro micrófono cuando realmente no lo necesitan para prestar su servicio. También deben especificarnos si van a acceder al micro solo para una función determinada, o si no especifican nada. Podrían utilizar la información recogida con fines comerciales o facilitársela a terceros. Puede que incluso esa app afirme no utilizar los datos obtenidos con ninguna finalidad, aunque las empresas a las que se los cede tal vez sí lo hagan.

Pero, si bien son muchas las personas que han comprobado cómo algunas de sus conversaciones se convierten después en anuncios publicitarios sobre los temas tratados en dichas conversaciones, el tema de los televisores en el salón de casa o en las habitaciones parece inquietar o sorprender más.

Cuando activamos el sistema de control por voz de un televisor de última generación, puede captar las conversaciones que se produzcan en la sala, e incluso pasárselas a terceras empresas. Como muestra un botón: en los televisores Samsung, cuando se habilita el reconocimiento de voz, se informa al usuario en la política de privacidad de lo siguiente: “Tenga en cuenta que si sus palabras habladas incluyen información personal u otra información confidencial, esa información estará entre los datos capturados y transmitidos a un tercero a través de su uso del reconocimiento de voz”[5].

5 https://www.samsung.com/hk_en/info/privacy/smarttv/

CEU

Colegios