kaspersky

Manual para padres ¿Cuándo dar el primer dispositivo a los niños?

1 ¿Qué debería hacer antes de dar un dispositivo a un niño?

- Restringe en la configuración las compras en las apps, ya que algunas aplicaciones gratuitas permiten compras de la app. Aquí encontrarás consejos útiles de cómo hacerlo.
- Instala todas las apps básicas que tu hijo pueda necesitar para comunicarse y aprender (mensajería, juegos educativos, aplicaciones del cole, etc.)
- Configura las opciones de privacidad de cada app. Descubre cómo hacerlo con nuestro Privacy Checker.
- Instala una solución de control parental.
- Define la clasificación por edad en la configuración de contenidos del dispositivo.
- Bloquea y restringe las llamadas de números desconocidos.

2 ¿Cómo introducir correctamente un dispositivo en la vida de los niños?

- Define una serie de normas de uso.
- Establece lugares y horas "libres de tecnología".
- Realiza actividades conjuntas que no dependan del uso de la tecnología.
- Limita el uso del dispositivo durante:

Comidas

Hora de acostarse

Salidas y eventos familiares

Deberes y estudio

Reuniones sociales

Actividades extraescolares y de ocio

Rutinas matinales

3 ¿Qué normas de seguridad online deberían conocer mis hijos?

- Establece unas normas claras de lo que pueden y no pueden hacer online.
- Enseña a los peques las normas básicas sobre privacidad y sobre los riesgos de la sobreexposición en Internet.
- Haz hincapié en que nunca deben compartir datos personales: dirección, escuela, contraseñas, geolocalización, etc. en Internet.
- Adviérteles de no crear usuarios y nicks con sus nombres o datos reales.

4 ¿Cuáles son los principales riesgos que he de contarles a mis hijos?

- Explícales qué son las estafas phishing[1] y porqué son peligrosas.
- Adviérteles de los riesgos de descargar juegos de páginas no oficiales y poco fiables.
- Enséñales a ignorar sitios con publicidad intrusiva, encuestas y sorteos. Las soluciones de seguridad pueden detectar estas páginas y bloquearlas.
- Enséñales a pensar dos veces antes de hacer clic en links y páginas sospechosas o antes de abrir un mail de desconocidos con algún enlace o adjunto. De nuevo, las soluciones de seguridad pueden ayudar a detectar y bloquear programas y archivos maliciosos.
- Enséñales y anímales a pedir ayuda si se sienten incómodos o sospechan de algo cuando están online.
- Ayúdales a elegir una contraseña única y anímales a cambiarla de forma periódica. Un gestor de contraseñas[2] puede ser un buen aliado en esta tarea.

[1] El phishing consiste en el envío de correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y bancaria al usuario. A través de un enlace incluido en el email, intentan redirigirlo a una página web fraudulenta para que introduzca su número de tarjeta de crédito, DNI, la contraseña de acceso a la banca online, etc.

[2] Los gestores de contraseñas son aplicaciones que sirven para almacenar todas nuestras credenciales (usuarios, contraseñas, sitios web a los que corresponden, etc.) en una base de datos cifrada mediante una contraseña "maestra". De este modo, podemos gestionar todas nuestras cuentas de usuario desde una misma herramienta, memorizando únicamente una contraseña.

5 Tengo miedo de que extraños contacten con mis hijos. ¿Qué debería decirles para prevenirles?

- Enséñales a no aceptar solicitudes de amistad de gente que no conozcan en la vida real.
- Explícales que si un extraño está tratando de averiguar información personal sobre ellos, su familia o sus amigos, deben comunicártelo enseguida.
- Construye una relación de confianza hablando con ellos de forma regular sobre sus experiencias online.

6 Mi hijo está siempre jugando online. ¿Hay riesgos también cuando juegan? ¿Cómo puedo prevenirlos?

- Permite que tu hijo juegue online, pero solo con personas que conozca, al menos al principio.
- Asegúrate de que tu hijo pueda crear un juego o servidor privados.
- Enséñales a descargar juegos solo de páginas oficiales y revisa el número de descargas y los comentarios que comparten otros usuarios.
- Anímales a ignorar los links que se comparten en los chats y no acceder a ellos, ni compartirlos.
- Considera instalar una solución de seguridad que incluya el "modo juego" y pueda detectar cualquier web de phishing y programas maliciosos.
- Enfatiza la importancia de no compartir sus contraseñas, ni siquiera con sus amigos.

7 Mi hijo sufre acoso en Internet. ¿Qué debo hacer?

- Mantén la calma, deja que tu hijo comparta sus sentimientos y los detalles del incidente sin interrumpirle.
- Asegúrate de que tu hijo se siente comprendido y a salvo.
- Antes de borrar los mensajes y bloquear al acosador, haz capturas de pantallas de todo el contenido.
- Avisa a tu hijo de que no debe contestar, sobre todo retando o con mensajes negativos.
- Plantéate actualizar la configuración de privacidad, las contraseñas y bloquea y reporta al acosador.
- Reporta el incidente a la escuela en caso de que sea un compañero o a las autoridades.
- Si tu hijo muestra signos de estrés, considera la posibilidad de pedir ayuda profesional.

8 Mi hijo acosa a otros en Internet. ¿Qué debería hacer?

- Mantén la calma, reúne pruebas y comprende el contexto en su conjunto.
- Habla de la situación con tu hijo para conocer su versión de los hechos.
- Ayúdales a entender el impacto de sus acciones. Pregúntales cómo se sentirían si estuvieran en el lugar de la víctima.
- Anímale a disculparse, ya sea directamente o a través de la mediación.
- Monitoriza el uso de la tecnología. Sin ser demasiado invasivo, controla sus interacciones online. Las aplicaciones digitales para padres pueden permiten monitorizar el historial de búsqueda.
- Reedúcale para que comprenda la importancia del comportamiento responsable online.
- Involucra a la escuela, consejero escolar, psicólogo o terapeuta para verificar si existen problemas subyacentes o factores estresantes que conduzcan a este comportamiento.

9 ¿Qué preguntas debería hacerle a mi hijo para saber si su experiencia online es segura?

- ¿Qué es lo más interesante que has visto o leído hoy en Internet?
- ¿Has encontrado algo que te resulte confuso o no hayas entendido mientras estabas en Internet?
- ¿Has jugado o chateado con gente que no conoces en persona? ¿Cómo ha sido?
- ¿Cómo decides qué compartir y qué mantener privado online?
- ¿Alguna vez te has sentido incómodo con algo mientras navegabas o interactuabas online?
- ¿Hay alguna nueva aplicación o web que hayas descubierto y que te guste usar? ¡Probémosla juntos!
- ¿Sabes qué hacer si alguien te envía un mensaje o una solicitud que te parezca extraña o inapropiada?
- ¿Qué opinas sobre los límites de tiempo frente a la pantalla? ¿Alguna vez has sentido que necesitas un descanso de tus dispositivos?
- ¿Alguna vez has visto a alguien siendo cruel online? ¿Cómo te sentiste y qué hiciste?

10 ¿Cómo debo monitorizar la actividad de mis hijos en Internet, sin invadir su privacidad?

- Habla con tus hijos de su experiencia online de forma regular.
- Pasa tiempo con ellos en Internet: ver vídeos juntos, jugar online o explorar nuevos canales y apps con ellos.
- Instala apps de control parental centradas principalmente en su seguridad.
- Explícales que hay ciertos controles instalados en sus dispositivos y el porqué.
- A medida que vayan creciendo, pasa de una monitorización estricta a un concepto más orientado al tutelaje o asesoramiento, guiándoles en el uso y comportamiento responsable de Internet.
- Mantente actualizado con las últimas tendencias y amenazas digitales. Comparte con ellos esta información de una manera que la entienda.

11 ¿Qué signos podrían indicar que el uso de sus dispositivos está creando efectos negativos en mi hijo?

- Deterioro del rendimiento académico.
- Reducción de la actividad física o social.
- Síntomas físicos como fatiga visual, alteraciones del sueño o mala postura.
- Cambios de comportamiento como mayor irritabilidad, aislamiento de amigos y familia.
- Descuido de responsabilidades y pérdida de interés en pasatiempos que antes disfrutaba.
- Indicadores emocionales como cambios de humor, aumento de la ansiedad, signos de depresión, baja autoestima, problemas de imagen y baja motivación.
- Problemas cognitivos como disminución de la capacidad de atención y pérdidas de memoria.

kaspersky