Digital Security
Progress. Protected.

saferkidsonline

Seguridad en Internet para niños: guía para padres

Vidas digitales

Muchos de nosotros en ESET somos padres como tú. Sentimos la necesidad de guiar a nuestros hijos por la vida y protegerlos de cualquier daño, pero hoy en día la responsabilidad es un reto tremendo.

Con dispositivos móviles cada vez más complejos, nuevas plataformas de comunicación y un lenguaje online que evoluciona rápidamente, los padres tenemos mucho que aprender para ayudar a nuestros hijos. Esta guía ofrece una ayuda y explica lo que hay que hacer para que tus hijos puedan utilizar Internet de forma segura.

¿Quién debería hablar con ellos?

No importa lo incómodo que te resulte, tienes que ser tú.

Tus hijos conocerán a muchas personas que desempeñarán papeles muy importantes en sus vidas, como familiares, amigos y profesores. Sin embargo, ninguno de ellos puede sustituir tu papel de padre. A los ojos de un niño, eres tú quien tiene todas las respuestas y es capaz de ayudarle si no está seguro de lo que tiene que hacer.

¿Cuándo deberías hablar con ellos?

¡Ahora!

Desde el primer momento en que un niño muestra interés por su tablet, smartphone u ordenador, hay que empezar a explicarle las cosas. Hay muchas reglas que enseñamos a los niños para mantenerlos seguros en el mundo real. Hay otras tantas para el mundo online. Aunque las amenazas inmediatas a la seguridad personal pueden presentarse de forma diferente, el potencial de daño es igual de real. A medida que tu hijo crezca, surgirán nuevos tipos de problemas y cambiarán los consejos pertinentes. Una buena y cariñosa orientación para las nuevas situaciones puede ser el paso decisivo que empuje a tu hijo en la dirección correcta.

Educación: un camino de dos direcciones

¿Sientes que tus hijos saben más de informática que tú? No estás solo.

Los niños de hoy en día son auténticos expertos en el uso de las nuevas tecnologías. Para muchos adultos son todo un reto y han de adquirir habilidades digitales. Sin embargo, saber cómo acceder a Internet no es lo mismo que utilizarlo con seguridad.

No es necesario que tú, como padre, sepas más que tus hijos sobre lo que ocurre en el mundo virtual. Pero debes tener el máximo control en caso de que tus hijos se encuentren con algo que no les resulte familiar y necesiten comentarlo con alguien más experimentado.

Lo importante es hacer que el niño forme parte del desarrollo del proceso: crear un entorno en el que pueda preguntar libremente y tener tiempo para absorber nueva información.

¿Qué deberías hacer cuando tu hijo está en "esa edad"?

Utiliza herramientas de control parental

Sea cual sea la edad de tus hijos, puedes aprovechar la tecnología existente. Las herramientas de control parental de ESET permiten bloquear sitios o incluso categorías de páginas que contienen material potencialmente ofensivo. Puedes establecer límites de tiempo para navegación por Internet o para jugar a juegos. Al mismo tiempo, permite que tu hijo te pida permiso para visitar ciertas páginas o tener más tiempo de juego, en caso de que tenga sus tareas escolares terminadas.

Además de las herramientas de control, tenemos algunos consejos para diferentes grupos de edad que harán más seguras las actividades online de los niños.

HASTA 10 AÑOS

1. Acompaña a los niños en sus primeras experiencias en la web

Asegúrate de estar presente cuando tus hijos den sus primeros pasos en el mundo digital. El primer contacto de un niño con Internet es una buena oportunidad para sentarse y guiarle en su nueva aventura.

2. Establece condiciones para el uso de Internet

Establece reglas básicas para el uso de Internet. Una buena práctica es supervisar el número de horas que se pasan conectados y establecer los horarios en los que se permite el acceso a la red.

3. Sé un buen ejemplo

Los niños suelen tomar como ejemplo el comportamiento de sus padres, tanto en la vida real como en Internet. Si los miembros de la familia se comportan de forma correcta, es muy probable que el niño siga el ejemplo.

DE 11 A 14 AÑOS

1. Enséñales a no compartir información que pueda identificarlos

Es importante dejar muy claro a los niños que en el mundo virtual no todo el mundo es amigo, y que algunas personas pueden incluso querer hacerles daño. Explícales por qué no es seguro compartir información como la dirección, el número de teléfono, el colegio o las actividades extraescolares a las que asisten. El niño también debe pedirte autorización antes de compartir fotos potencialmente sensibles en Internet.

2. Mantén un diálogo abierto

Anima a tus hijos a ser abiertos contigo y a preguntar libremente sobre lo que ven en Internet. Si utiliza un ordenador de sobremesa, intenta instalarlo en una habitación en la que pase toda la familia y donde pueda estar bajo tu supervisión, no en su dormitorio.

DE A 15 A 18 AÑOS

1. Nadie más debería conocer sus contraseñas

Sabemos que los adolescentes pueden ser difíciles, pero asegúrate de que entienden y ejercen las mejores prácticas cuando se trata de contraseñas. Respeta la privacidad de tus hijos adolescentes, pero al mismo tiempo asegúrate de que nunca den una copia de sus contraseñas a un extraño, o que se las presten a otra persona, físicamente o por Internet.

2. Denuncia inmediata del acoso y el ciberacoso

¿Recuerdas al matón del colegio? ¿El niño grande que les hacía la vida imposible a los demás? Hoy en día, muchos matones se han pasado a la tecnología moderna y se esconden detrás de Internet. Lo que no ha cambiado es el hecho de que intentan dañar psicológicamente a los demás. Por ello, hay que decir a los niños que informen inmediatamente a sus padres si alguna vez sufren acoso escolar.

3. Las transacciones financieras online son solo para adultos

Comprar algo en Internet no debería ser un problema, siempre que se haga con cuidado. Hasta que los niños comprendan las medidas de precaución necesarias que deben tomarse al enviar información financiera personal, deben hacerlo únicamente bajo la supervisión de sus padres.

¿Cuáles son las principales amenazas online?

Malware

"Malware" es la abreviatura de software malicioso. Este tipo de aplicaciones intentan dañar un dispositivo de varias maneras. Algunos de ellos cifran los archivos de tu ordenador, otros intentan espiarte o descargar otras aplicaciones peligrosas en tu equipo.

En la mayoría de los casos, la infección se produce debido a "errores" cometidos por los usuarios tras ser engañados por el atacante. La aplicación de soluciones de seguridad de confianza y buenas prácticas reducen el riesgo de ser infectado por este tipo de código malicioso.

Spam

Ya conocerás el spam. Son todos esos "correos basura" no solicitados que aparecen en tu bandeja de entrada. Estos mensajes suelen incluir publicidad que te invita a visitar determinadas páginas con ofertas "milagrosas", que en su mayoría albergan contenidos potencialmente dañinos.

Scam

Las estafas son actos de engaño realizados a través de Internet. Inicialmente pueden adoptar muchas formas, como el spam y el uso de técnicas de ingeniería social. En este último caso, los atacantes ofrecen vender algo, actuar como tus amigos o incluso hacerse pasar por tu banco, mientras que lo único que quieren es obtener información confidencial. Los mensajes falsos en los que se solicitan nombres de usuario y contraseñas de redes sociales son también un ejemplo de estafa muy frecuente.

Cyberbullying

Este comportamiento hostil suele dirigirse a los niños. La víctima puede ser amenazada y humillada por sus compañeros en el entorno cibernético y es frecuente entre los adolescentes. Puede perjudicar al niño, causándole un trauma emocional. El ciberacoso tiene muchas vías: incluso se pueden utilizar las funciones de chat de los juegos de consola.

Grooming

El Grooming ocurre cuando un adulto intenta persuadir a un niño para que realice actividades sexuales. El adulto intenta crear un ambiente de confianza y establecer una conexión emocional con el niño. El adulto a menudo se hace pasar por niños para establecer una relación cercana y así ganarse la confianza del niño, y luego trata de concertar una cita en persona. Por eso es tan importante que, como padre, sepas con detalle con quién se relaciona tu hijo cuando está conectado a Internet.

Sexting

"Sexting" deriva de "sex" y "texting" y existe desde hace tiempo. Si bien la función SMS se utilizaba en teléfonos móviles para intercambiar mensajes de texto, el desarrollo de los correos electrónicos y otros servicios de mensajería hizo que también se pudieran enviar fotos y vídeos. Es una práctica habitual, ya que la mayoría de los adolescentes y niños llevan sus dispositivos móviles consigo en todo momento.

Information Theft

La información enviada a través de la web, sin las precauciones necesarias, puede ser interceptada por terceros. La información obtenida de este modo puede utilizarse para fines como el robo de identidad o el chantaje.

Últimas recomendaciones

Utiliza herramientas de control parental

El control parental puede utilizarse en los navegadores y en los programas antivirus. Se puede encontrar en la última versión de ESET Smart Security o también como la aplicación independiente ESET Parental Control para Android. Este tipo de herramientas también están disponibles para las videoconsolas.

No dejes que tu hijo envíe información confidencial a través de Internet

Nunca se debe solicitar información sensible por correo electrónico o por chat. Los bancos no solicitan los datos de tu cuenta o tu PIN de esta manera. También es importante no dar información tan importante a tus hijos.

No respondas ni elimines los mensajes de acoso

Si tu hijo es víctima de ciberacoso, no deberías tomar represalias. Explícale que el acosador quiere provocar una reacción, ya que eso alimenta su deseo de hacer daño a los demás. Si este tipo de situación sigue ocurriendo, notifica a las autoridades competentes. No borres ningún mensaje recibido ya que podría ser utilizado como prueba.

Mantente al día

Hoy en día, negar a tu hijo el acceso a las tecnologías no es una solución. Los dispositivos digitales forman parte de su vida cotidiana y son cada vez más importantes para su desarrollo. En lugar de poner restricciones, ayuda a tus hijos a utilizarlos de forma segura y participa en la interacción entre el niño y el dispositivo. También conviene señalar que muchos de estos riesgos pueden afectar también a los adultos, y que muchas de las precauciones aquí descritas deben tomarse a cualquier edad.

La seguridad de los niños es responsabilidad de todos y los consejos que se ofrecen en esta guía son únicamente los básicos. Para más información, visita nuestros sitios web y páginas en las redes sociales.

www.eset.com
www.welivesecurity.com
Síguenos en: www.facebook.com/eset
https://twitter.com/ESET @ESET