Guía para Padres preocupados por el uso seguro de las redes sociales

ENJOY SAFER TECHNOLOGY™

Introducción

No ha pasado tanto tiempo desde que los niños solían jugar en la calle y solo volvían a casa cuando tenían hambre. Sin embargo, la eclosión de Internet lo ha transformado todo. Hoy en día, los jóvenes prefieren la realidad virtual de las redes sociales.

En ESET también somos padres y entendemos las preocupaciones que tienes al ver a tus hijos absorbidos por el cibermundo. Por ese motivo hemos confeccionado esta guía. En ella encontrarás información sobre las amenazas que les acechan en las redes sociales y posibles soluciones que te ayudarán a mantener a tu familia protegida.

1. ¿Quién debería hablar con ellos?

No importa lo incómodo que te haga sentir, tienes que ser tú.

A lo largo de su infancia, tus hijos conocerán a gente que tendrán un papel muy importante en su vida, como familiares, amigos y profesores.

Aun así, ninguno de ellos puede sustituir tu papel como padre. En los ojos de un niño, tu eres quien tiene todas las respuestas y puedes ayudarles si no saben qué hacer.

2. ¿Cuándo deberías hablar con ellos?

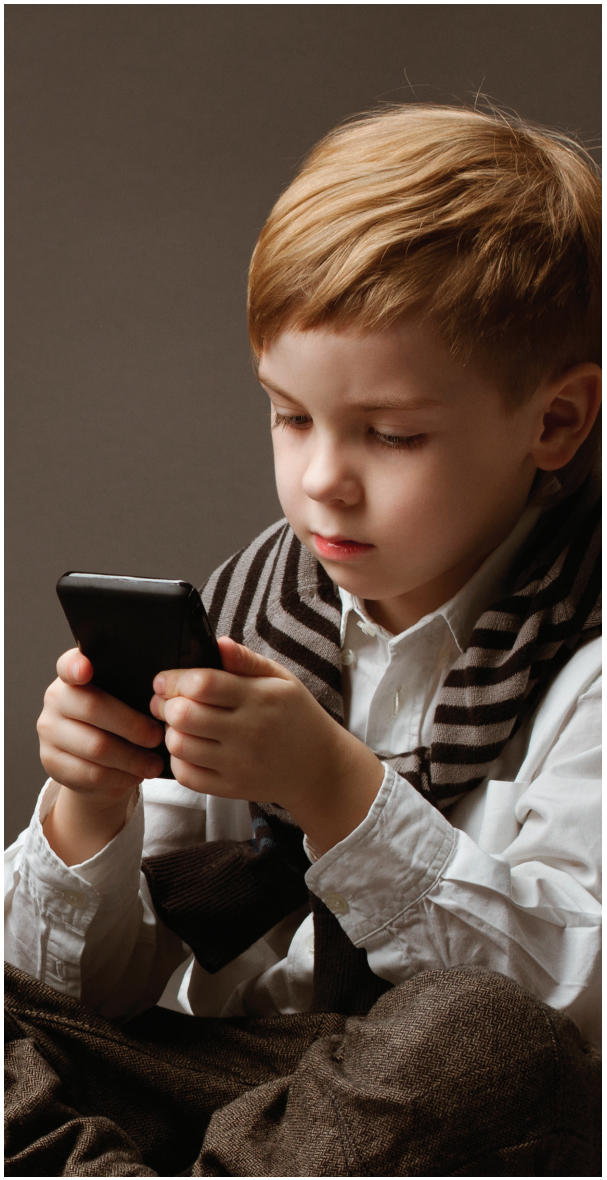
Ahora. O cuanto antes, mejor.

A medida que tu hijo va creciendo, van surgiendo nuevos problemas. Un buen consejo en cualquiera de estas nuevas situaciones puede ser un paso decisivo, que llevará a tu hijo por la buena dirección en el futuro.Esto es especialmente cierto, cuando hablamos de ciberespacio.

Desde el momento en que un niño muestra algún interés por tu tablet, smartphone u ordenador o por internet en general, deberías empezar a explicarle que todo lo aprendido sobre seguridad, es aplicable también para internet. En otras palabras, cambian los medios, pero las amenazas siguen siendo las mismas.

3. ¿Qué hacer cuando mi hijo tiene esa edad?

A continuación, compartimos un conjunto de herramientas básicas para que los niños naveguen más seguros:



HASTA LOS 10 AÑOS

1. “Acompáñales durante sus primeras experiencias en internet”

Asegúrate de que estás allí cuando tus pequeños dan sus primeros pasos. El primer contacto de un niño con internet es una buena oportunidad para sentarse con él y guiarle en su nueva aventura.

2. “Establece las condiciones para utilizar internet”

Establece las reglas básicas para usar internet. Una buena práctica es supervisar el número de horas que está conectado y establecer horas en las cuales está permitido conectarse.

3. “Sé un buen ejemplo para él”

Los niños normalmente toman el comportamiento de sus padres como ejemplo, y esta regla se aplica tanto para internet como para la vida real. Si los miembros de la familia tienen un comportamiento adecuado, esto pasará inmediatamente al niño.

DE 11 A 14 AÑOS

1. “Usa herramientas de control parental”

Aprovéchate de la tecnología actual y utilízala a tu favor. Las herramientas de ESET Parental Control permiten bloquear páginas web o incluso categorías de páginas web que contienen material potencialmente ofensivo, te permiten establecer límites de tiempo para navegar por internet o incluso juegos. Al mismo tiempo, le dan la oportunidad a tu hijo de pedir permiso para visitar ciertas páginas o tener más tiempo para jugar, si tiene los deberes terminados.

2. “Enséñales a no compartir información que pueda identificarles”

Es importante explicarles claramente a los niños que en el mundo virtual no todo el mundo son “buenos amigos” y que algunos tal vez quieran 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 acuden. El niño o niña también debería pedirte autorización antes de compartir imágenes potencialmente sensibles en internet.

3. “Mantén un diálogo abierto”

Anima a tus hijos a ser abiertos contigo y a preguntar libremente sobre lo que ven en internet. Si es posible, instala el equipo en una habitación que sea un punto de reunión de la familia y pueda estar bajo tu supervisión, no en su propia habitación.

DE 15 A 18 AÑOS

1. “Nadie debería saber sus contraseñas”

Sabemos cómo son los adolescentes y que pueden ser difíciles en ocasiones, pero asegúrate de que entienden las buenas prácticas cuando hablamos de contraseñas. Al fin y al cabo, son como sus llaves de casa. Respeta la privacidad de los adolescentes, pero al mismo tiempo asegúrate de que no dan una copia de sus contraseñas a extraños, o las piden a otros ni en persona ni por internet.

2. “Informa inmediatamente del stalking y cyberbullying”

¿Te acuerdas de los líderes de tu clase? El chico grandote que le hacía la vida realmente difícil a los raros de la clase? Hoy en día, muchos de ellos se han pasado a la tecnología y se ocultan detrás de internet. Lo que no ha cambiado es el hecho de que intentan hacer daño psicológico a los demás. Por esto, deberíamos decir a los niños que informen inmediatamente a sus padres si alguna vez sufren algún tipo de acto de este tipo.

3. “Las transacciones financieras online son solo para adultos”

Comprar algo por internet no debería ser un problema, siempre y cuando se realice cuidadosamente. Hasta que los niños entiendan las medidas de precaución necesarias que deben tomarse cuando se envía información financiera personal, solo deberían realizarlo bajo la supervisión de sus padres.

4. ¿Qué debemos vigilar?

Malware

Es la abreviación inglesa de los términos malicioso y software, en otras palabras, códigos maliciosos. Los virus, gusanos y troyanos son algunos de los ejemplos más conocidos y sus ataques a los usuarios, sin restricciones de edad, han sido documentados ampliamente.

Uno de ellos –el gusano Koobface- se propagó por Facebook en 2009. Usando mensajes atractivos hacía que los equipos de sus víctimas pasaran a formar parte de una botnet (red de ordenadores zombi que puede ser controlada remotamente por el atacante). Su versión más novedosa, que apareció unos dos años después, era mucho más avanzada, infectando a los usuarios de la red social sin importar el sistema operativo que utilizaban (Windows, Mac o Linux).

Phishing

La mayoría de atacantes utilizan este método para robar información confidencial como las credenciales de acceso para el perfil de las redes sociales de tu hijo. Esto se lleva a cabo normalmente mediante un correo electrónico con un enlace a una réplica de la página web de la red social o de cualquier otra página que suplantan. Puede ser bastante difícil identificar la página web falsa puesto que las diferencias a menudo son mínimas y los menores engañados puede que inserten información sin darse cuenta de que hay algo incorrecto.

Robo de identidad

Asegúrate de que tus hijos no publiquen información confidencial como la dirección de la casa, el número del móvil, el colegio o la clase a la que asisten, el cumpleaños o cualquier otra fecha, puesto que podrían ser utilizados para identificarles. El motivo es el robo de identidad, una de las formas más propagadas de cibercrimen, donde los criminales obtienen tu información personal y la utilizan para suplantar tu identidad o incluso la de tu hijo con propósitos maliciosos.

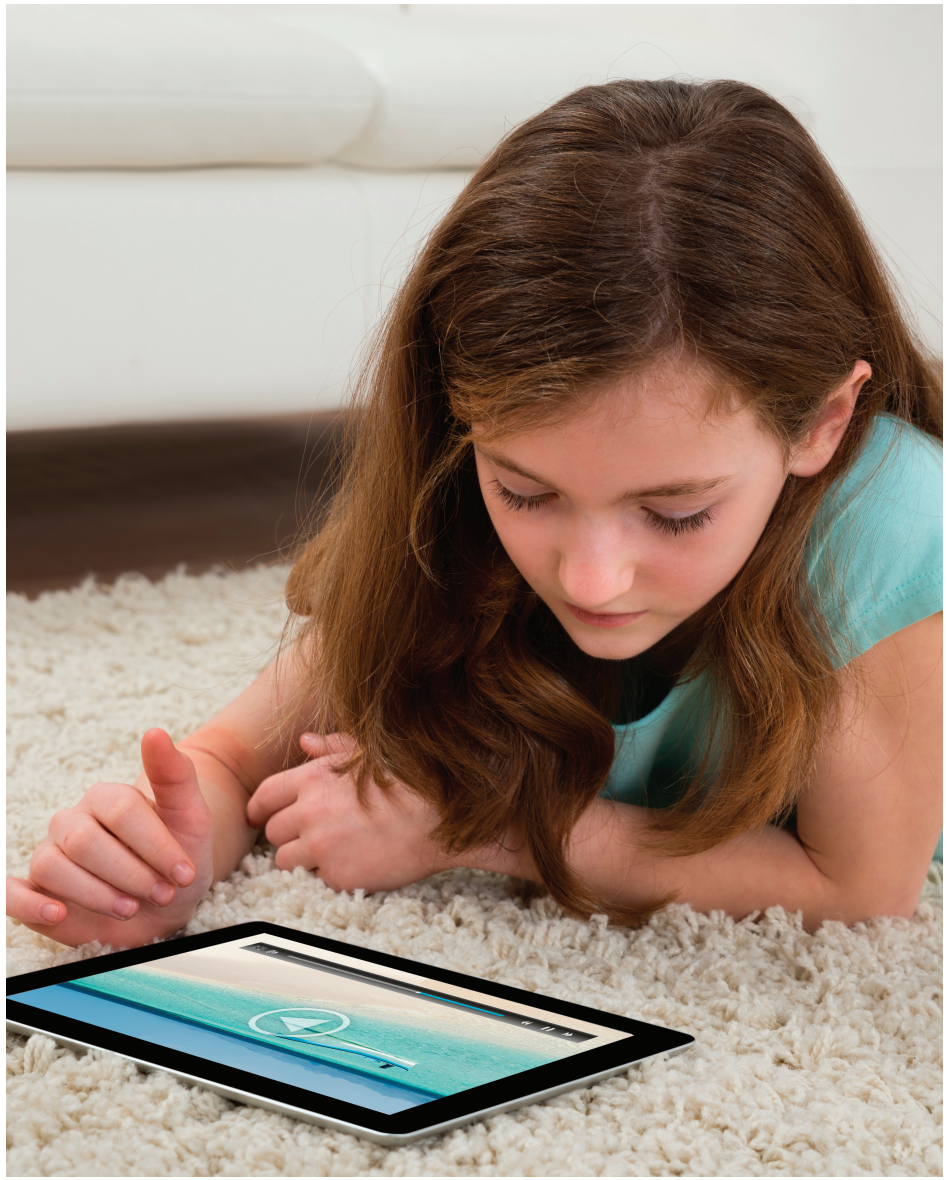
Existen básicamente dos formas en las que el atacante puede conseguir esta información confidencial:

Usando ingeniería social, fingiendo ser un amigo de tu hijo o un chico de su misma edad, e intentando extraer información personal por esta vía.

Debido a una mala configuración de la red, puede que haya demasiada información accesible públicamente en el perfil de la red social de tu hijo. Es importante tener en cuenta que esto no es solo un problema de los jóvenes sino también de muchos usuarios adultos que no son conscientes de los riesgos.

Cyberbullying

No todas las amenazas a las que pueden enfrentarse tus hijos en las redes sociales implican a cibercriminales. Sus colegas también pueden ser un problema. Decimos esto porque el bullying ya no es un problema únicamente de clases y colegios. Hoy en día también se da en el ciberespacio, haciéndose más peligroso que nunca.



Grooming

Otro riesgo es el grooming, especialmente dirigido a niños más jóvenes. Se trata de un adulto que finge ser un niño para poder ganarse su confianza fácilmente y convencerle para realizar actividades sexuales. Esto está relacionado de muchas formas con el sexting, que incluye mensajes con contenido inapropiado que podrían ser intercambiados por tu hijo.

Sexting

El 'sexting' viene del acrónimo de Sexo y Texting. Inicialmente, como su nombre indica, hacía referencia a correos electrónicos que contenían mensajes eróticos. Posteriormente, debido al progreso tecnológico, ha evolucionado e incluye el intercambio de imágenes y vídeos, y se ha convertido en una práctica común puesto que la mayoría de adolescentes y niños tienen sus móviles y dispositivos con ellos la mayor parte del tiempo.

Spam

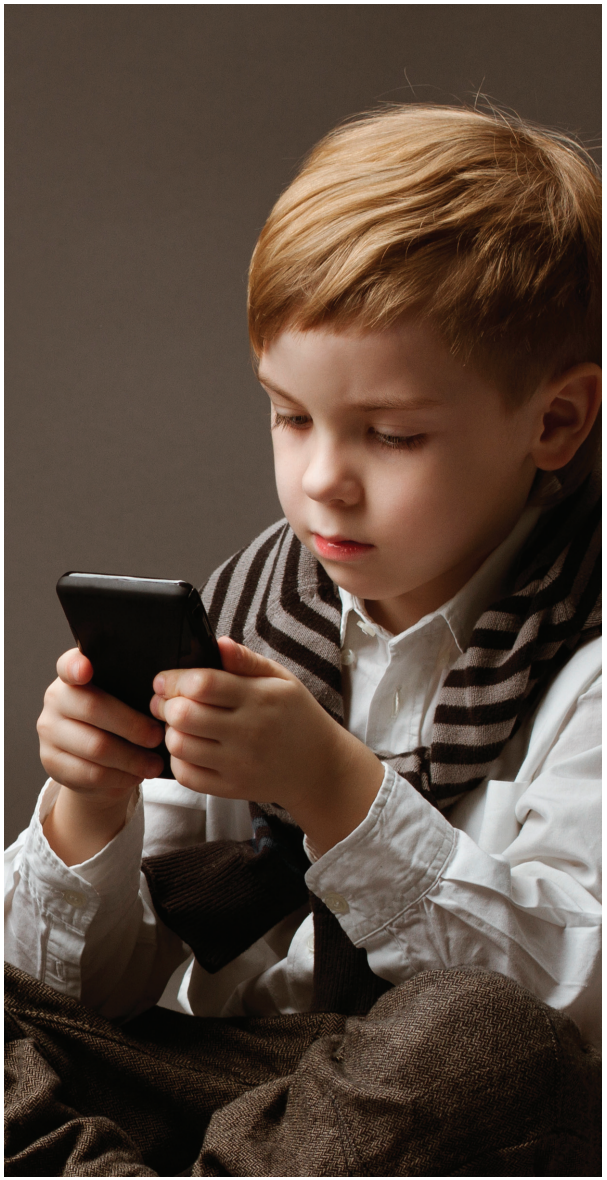
Ya sabes qué es el correo basura. Son todos aquellos correos no solicitados que llenan tu bandeja de entrada a diario. Normalmente este tipo de mensajes incluyen anuncios que te invitan a visitar ciertas páginas con ofertas "milagro", la mayoría de ellas albergan contenido potencialmente malicioso.

Scam

Los 'scam' son actos engañosos llevados a cabo por internet. Pueden ser de muchas formas diferentes, como el correo basura o el uso de técnicas de ingeniería social. En este último caso, los atacantes ofrecen vender algo, actúan como colega tuyo o se personan como tu banco, mientras que lo único que quieren es obtener información confidencial. Los mensajes falsos que solicitan el usuario y contraseña de nuestra red social de internet también se consideran frecuentemente como un ejemplo de scam.

5. ¿Qué medidas puedo tomar?

En este escenario de amenazas, el uso de redes sociales parece ser una actividad realmente peligrosa. Sin embargo, prohibir a tu hijo que las utilice no va a solucionar el problema, probablemente sólo conseguirías que intentara eludir las reglas que establezcas. Pero no te preocupes, aquí tienes algunos consejos que harán más seguro el uso de las redes sociales y que proporcionarán una protección adecuada para tus hijos y tu familia.



Habla con ellos

El diálogo es una de las partes más importantes para mantener a tus hijos seguros en Internet, especialmente cuando hablamos de redes sociales. Mantener la comunicación y tu mente abierta a preguntas y al debate es crucial si quieres que tus hijos confíen en tu opinión y sigan tu consejo.

Un buen ejemplo de ello es el ciberacoso y su prevención. Explica claramente a tus hijos que si detectan un comportamiento así, incluso si no les afecta directamente, deberían informarte inmediatamente a ti o a sus profesores o tutores (dependiendo de dónde haya sucedido). Es importante tener en cuenta que nunca deben borrar el mensaje de acoso puesto que es la única prueba que tenéis.

- **No contestes ni elimines los mensajes de acoso**

Si tu hijo es víctima del ciberacoso no debería contraatacar. Explícale que el atacante quiere provocar este tipo de reacción puesto que alimenta sus deseos de hacer daño. Si te encuentras con este tipo de situaciones y si ocurren de nuevo, debes informar a las autoridades correspondientes. Sin embargo, nunca borres ningún mensaje recibido puesto que son pruebas del acto delictivo.

Utiliza un producto de control parental

Dependiendo de la edad de tus hijos deberías utilizar un producto de control parental. **ESET Smart Security** te permite configurar una lista de páginas web bloqueadas y también restringir el rango de tiempo y el número de horas que pueden pasar conectados a Internet.

Por otra parte, los niños también deberían poder expresarse. La aplicación **ESET Parental Control para Android** les permite pedir permiso para acceder a una determinada página web o tiempo adicional al que tu hayas establecido para su red social, en caso de que hubieran terminado todas sus tareas y deberes antes de lo esperado.

Utiliza un producto de seguridad fiable

Como el malware es una de las amenazas más propagadas por el ciberespacio, instalar un producto antivirus con detección proactiva y una base de firmas actualizada es esencial para evitar infecciones cuando utilicen las redes sociales.

Las herramientas antispam y el cortafuegos también hacen que la optimización de la seguridad del sistema sea óptimo para enfrentarse a estos riesgos. Por otra parte, tu hijo no debería usar una cuenta de administrador cuando utilice las redes sociales. Configura un perfil especial de usuario para tus hijos para minimizar el impacto de las incidencias de seguridad.

Configura el uso de https

Comprueba que tu hijo navega por protocolo seguro https (puedes verlo en la barra de navegación) cuando utilice redes sociales.

Con ello contribuirás a evitar los ataques de escuchas ilegales en información de texto legible. Mientras utilizas el protocolo https, toda la información –no solo las credenciales de usuario y contraseña de tu pequeño- será cifrada e ilegible para cualquier ataque malicioso.

Aconseja a tus jóvenes que utilicen esta configuración útil cuando accedan a redes sociales desde Wi-Fi públicas.

- **No permitas que tu hijo envíe información confidencial por internet**

Nunca deberían solicitarte información confidencial por correo electrónico o en un chat. Los bancos nunca solicitan tu número de cuenta y mucho menos tu número PIN de esta forma. También es importante no proporcionar esa información a tus hijos.

- **No todo lo que ves en internet es verdad**

No toda la información que puedes encontrar en internet procede de una fuente fiable y es importante que tu hijo conozca esta diferencia. Crea un blog donde puedas publicar tu opinión para demostrar qué fácil es adquirir un espacio en internet y manipular el contenido.

Utiliza contraseñas fuertes y autenticación de doble factor

¿Tus hijos saben cómo es una contraseña segura? Comprueba que no utilicen opciones fáciles de adivinar como "contraseña" o "12345". Además, debería contener al menos 10 caracteres, mayúsculas y minúsculas, números y símbolos especiales como # O @. También, recuérdales que no proporcionen la contraseña a nadie, ni a sus mejores amigos.

Si se conectan a Facebook, Twitter u otras redes sociales populares, comprueba que tus hijos utilicen autenticación de doble factor, disponible en los ajustes de seguridad. Recibir un código de un solo uso en su smartphone añade una capa de seguridad más que es difícil de quebrantar por los atacantes. Muestra a tus hijos cómo administrar su perfil utilizando el Registro de actividad, revisando sus acciones y las de otros que están conectados con ellos.

- **Si publicas algo en internet, permanece para siempre**

Enséñales a tus hijos que cualquier cosa que se publica en internet, permanece para siempre. Y además al hacerlo, pierden el control sobre ello ya que puede ser compartido por cualquiera, incluso por extraños. Una buena regla de oro es no compartir ninguna foto, estado u otro contenido que no quisieran que tú, como padre, o la abuela vieran.

Esto se aplica a todas las formas de presencia online: redes sociales, mensajería instantánea, blogs o comentarios.

Configura la privacidad de tus redes sociales

Los ajustes de privacidad predeterminados de las redes sociales no garantizan la seguridad de tu hijo. Por tanto, es aconsejable dedicar un poco de tiempo para configurarlo y también comprobar qué información podría filtrarse.

- **Facebook**

Comprueba que ningún ajuste del perfil de tu hijo está disponible públicamente, sin excepciones. Preferiblemente, haz que la información esté disponible solo para sus amigos y, si es posible, solo para un pequeño grupo de ellos (tales como familia o amigos cercanos) si son demasiados.

Limita la audiencia que puede ver las imágenes, el estado y otros contenidos donde tu hijo puede ser etiquetado. Evita las aplicaciones que pueden acceder a su información personal o a publicar en su muro.

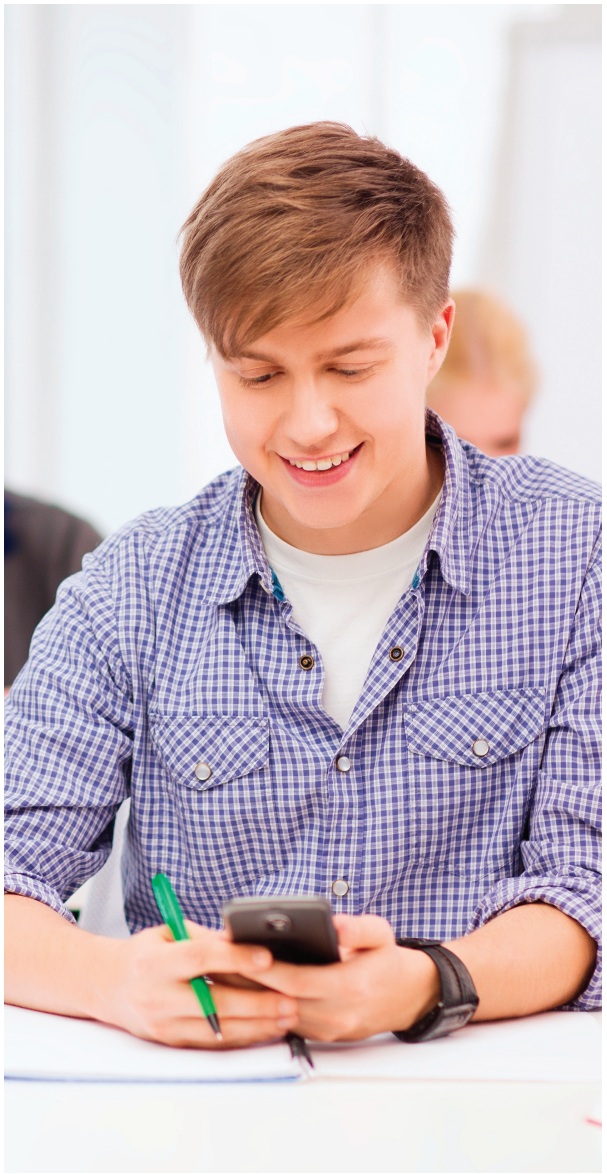
Enséñales a que solo acepten peticiones de amistad de personas que conocen personalmente. Explícales que contactar con extraños en el ciberespacio puede ser tan peligroso como hacerlo en el mundo real.

- **Twitter**

Twitter tiene sus propias características específicas, tales como el límite de 140 caracteres por tuit o el uso frecuente de enlaces acortados. Es en estas diferencias donde deberías centrarte para explicarles a tus hijos cómo protegerse.

Además de consejos como solo seguir a gente que conozcan o evitar enlaces sospechosos, también deberían comprobar la legitimidad de cualquier mensaje recibido sobre el que pueda haber dudas. Una forma de comprobar si es malicioso es buscarlo (integra o parcialmente) en la red. Lo más probable es que alguien ya haya descubierto el engaño y lo haya publicado.

También, puedes instalar un complemento en el navegador de su equipo o dispositivo que soluciona el problema de los enlaces acortados y permite que tus hijos vean el enlace original sin tener que hacer clic en él.



5 consejos más para padres

1. Asigna una cuenta de usuario a tu hijo. Este es el primer paso para controlar eficazmente su actividad en internet. El papel del administrador de sistemas siempre debería realizarlo un adulto.

2. Mantén tu antivirus y herramienta de control parental actualizados.

3. Controla su historial de navegación. Es importante establecer esto de muto acuerdo.

4. Controla la cámara web y asegúrate de que está desconectada o cubierta (si está integrada) cuando no está siendo usada.

5. Revisa los ajustes de configuración de las redes sociales que tu hijo utiliza. Un perfil que puede compartirse públicamente sin limitaciones puede poner en riesgo la integridad de una persona.

Decálogo de seguridad para el ciberespacio

Si quieres recordar la mayoría de consejos explicados en esta guía, puedes aplicar este decálogo más corto y simple:

1. Evita enlaces sospechosos
2. Nunca accedas a páginas web de dudosa reputación
3. Actualiza el sistema operativo y las aplicaciones
4. Descarga aplicaciones solo desde sitios web oficiales
5. Utiliza productos de seguridad
6. Evita introducir información personal en formularios dudosos
7. Ten cuidado con los resultados de los navegadores web
8. Solo acepta contactos conocidos
9. Evita ejecutar archivos sospechosos
10. Utiliza contraseñas fuertes

Conclusión

Sin duda las redes sociales son un recurso muy valioso para los usuarios de Internet. Aunque, como esta guía demuestra, existen muchas amenazas a las que pueden estar expuestos los niños cuando las utilizan. Por tanto, no subestimes a los cibercriminales y otros agentes maliciosos y haz un buen uso de las herramientas informáticas para proteger a las personas que más quieres.

Ayudarles a configurar sus perfiles de redes sociales apropiadamente y proporcionarles consejos simples y útiles puede ser decisivos para mantenerles seguros.


www.eset.es


www.facebook.com/ESET.Espana


https://twitter.com/ESET_ES