



Digital Security
Progress. Protected.

safer**kids**online

Guía para padres sobre las redes sociales

Introducción

¿Recuerdas la época en que los niños jugaban al aire libre y solo volvían a casa cuando tenían hambre? Internet lo ha cambiado todo. Hoy en día, los jóvenes pueden pasar horas cada día en las redes sociales.

Muchos de nosotros en ESET también somos padres, así que entendemos las preocupaciones que tienes al ver a tu hijo absorto en el mundo online. Por eso hemos elaborado esta guía. En ella encontrarás información sobre las posibles amenazas que acechan en las redes sociales y soluciones que te ayudarán a mantener a tu familia protegida.



1. Qué hay que vigilar

Malware

El malware es una combinación de dos términos, "malicioso" y "software", es decir, un código dañino. Los virus, gusanos y troyanos son algunos ejemplos. Los estafadores utilizan las redes sociales para inducir a los usuarios a descargar programas maliciosos, a menudo prometiendo software pirata o juegos.

Phishing

El término "phishing" deriva de "fishing" (pesca), ya que se utiliza como cebo para atrapar a las víctimas. Muchos ciberdelincuentes utilizan este método para robar información sensible, como las credenciales de acceso al perfil de la red social de un niño. Suele hacerse a través de un correo electrónico vinculado a una réplica del sitio web de una red social. Puede ser bastante difícil identificar una página falsa, ya que las diferencias suelen ser mínimas y los niños pueden insertar información personal sin darse cuenta de que algo va mal.

Robo de identidad

Asegúrate de que tus hijos no publican información sensible, como la dirección de tu casa, la del colegio, el número de teléfono o la fecha de nacimiento, que podría utilizarse para identificarlos. El robo de identidad es una forma de ciberdelincuencia muy extendida, en la que los delincuentes obtienen la información personal de los usuarios y la utilizan para hacerse pasar por ellos con fines maliciosos.

Hay dos formas principales mediante las cuales el atacante puede obtener estos datos sensibles:

Utilizar la ingeniería social, a menudo haciéndose pasar por el amigo de tu hijo.

Utilizar la información que es de acceso público en un perfil de red social y seleccionar la configuración de privacidad adecuada es crucial.

Abuso y acoso online

No todas las amenazas para tus hijos en las redes sociales tienen que implicar a los ciberdelincuentes. Sus compañeros también pueden ser un problema. El acoso no solo ocurre en los colegios: hoy en día se produce en Internet y puede ser tan dañino como en la vida real.

Otro riesgo grave es el grooming, especialmente cuando se trata de niños pequeños. El grooming consiste en que un adulto intente ganarse la confianza de un niño y entablar una relación con él para persuadirle de que realice actividades sexuales. Esto incluye a menudo el sexting (mensajes con contenido inapropiado que pueden ser enviados a tu hijo).

2. ¿Qué medidas puedes tomar para proteger a tus hijos?

Teniendo en cuenta las posibles amenazas, el uso de las redes sociales puede parecer una actividad peligrosa. Sin embargo, prohibir a tu hijo que las utilice no va a solucionar el problema. Encontrarán la forma de conseguir lo que quieren. A continuación encontrarás consejos que harán más seguro el uso de las redes sociales y proporcionarán una protección adecuada a tus hijos y a tu familia.

Hablar

El diálogo es una de las partes más importantes para mantener a tus hijos seguros en Internet, especialmente cuando hablamos de redes sociales. Mantener una comunicación abierta y honesta con tus hijos es crucial si quieres que confíen en tu criterio y sigan tus consejos.

Un buen ejemplo es el ciberacoso y su prevención. Deja claro a tu hijo que si alguna vez se encuentra con un comportamiento de este tipo, aunque no le afecte directamente, debe comunicarlo inmediatamente a alguien: a ti, a su profesor o a otros adultos responsables.

Utilizar software de control parental

Dependiendo de la edad de tus hijos, utiliza un software de control parental. ESET Smart Security te permite establecer una lista de sitios web bloqueados y restringir las horas en las que tu hijo puede estar conectado.

Sin embargo, los niños también deben tener su opinión. Por eso, ESET Parental Control para Android les permite pedirte permiso para visitar sitios web específicos o tener tiempo adicional en las redes sociales, quizás si han terminado las tareas o los deberes antes de lo previsto.

Utilizar una solución de seguridad fiable

Dado que el malware es una de las amenazas más extendidas en el ciberespacio, la instalación de una solución de seguridad con capacidad de detección proactiva en los dispositivos de tus hijos es esencial para evitar infecciones al utilizar las redes sociales.

Las herramientas antispam y de cortafuegos también permiten optimizar la seguridad del sistema frente a estos riesgos. Además, tu hijo nunca debe utilizar una cuenta de administrador cuando navegue por las redes sociales. Configura un perfil de usuario especial para tus hijos para minimizar el impacto de los incidentes de seguridad.

Utiliza contraseñas seguras y verificación de doble factor

¿Sabes tus hijos cómo es una contraseña segura? Asegúrate de que no utilicen opciones fáciles de predecir como "contraseña" o "12345". Debe tener al menos 10 caracteres, contener mayúsculas y minúsculas, un número y un símbolo especial como # o @. Adaptar una frase o la letra de una canción puede ayudar:

Mary tenía un corderito se convierte en Maryrteniauncorderito1@mb

Además, recuérdales que no deben compartir sus contraseñas con nadie, ni siquiera con sus mejores amigos.

Si te conectas a Facebook, Twitter u otras redes sociales populares, asegúrate de que tus hijos utilicen la verificación de doble factor que se ofrece en la configuración de seguridad. Recibir un código de acceso de un solo uso en tu smartphone añade otra capa de seguridad difícil de descifrar para los atacantes.

Cambiar la configuración del perfil a "privado"

La configuración de privacidad por defecto de las redes sociales no garantiza la seguridad de tu hijo. Por ello, es aconsejable dedicar algo de tiempo a configurarlas bien y a comprobar qué información podría filtrarse. Usemos Facebook como ejemplo:

Facebook

Utiliza la configuración del perfil para asegurarte de que nada se comparte con todos los usuarios. Preferiblemente, haz que la información esté disponible solo para tus amigos y familiares, y si es posible, solo para grupos reducidos (como la familia cercana o los mejores amigos).

Limita el público que puede ver las fotos, estados y otros contenidos en los que tu hijo ha sido etiquetado. Evita que las aplicaciones accedan a su información personal o publiquen en su muro.

Enséñales a aceptar solamente las solicitudes de amistad de personas que conozcan personalmente. Deja claro que hablar con desconocidos o contactar con ellos en Internet puede ser tan peligroso como encontrarse en el mundo real.

Para obtener información detallada sobre el uso de la configuración de Facebook, lee nuestro blog: <http://blog.eset.com/2011/05/25/facebook-privacy>

Twitter

Twitter tiene sus propias consideraciones específicas, como el límite de 280 caracteres, o el uso frecuente de URLs acortadas. Son estas diferencias las que también debes abordar cuando expliques a tu hijo cómo mantenerse seguro.

Además de seguir únicamente a las personas que conocen y evitar los enlaces sospechosos, también deben comprobar la legitimidad de cualquier mensaje que reciban. Los mensajes maliciosos suelen identificarse por otros usuarios y por la información compartida, por lo que una búsqueda rápida utilizando parte del mensaje puede ayudar.

Además, instala en tu ordenador o dispositivo un complemento del navegador de confianza que permita a tus hijos ver el enlace original de una dirección de URL corta sin tener que hacer clic en él.

Otras redes sociales

Hay muchas redes sociales que responden a diferentes intereses y grupos de edad. Es importante que compruebes que tus hijos utilizan las que son apropiadas para ellos. Disponemos de guías en vídeo sobre Snapchat, Instagram y YouTube, y también hemos elaborado una lista de redes sociales apropiadas para los niños.



3. Conclusión

Las redes sociales pueden ser un recurso valioso para los usuarios de Internet. Sin embargo, como demuestra esta guía, hay muchas amenazas a las que los niños pueden estar expuestos al utilizarlas. No subestimes a los ciberdelincuentes ni a otros autores malintencionados. Es esencial aplicar las mejores prácticas y utilizar herramientas de seguridad fiables para proteger a las personas importantes de tu vida.

Ayudarles a configurar correctamente sus perfiles en las redes sociales y ofrecerles consejos sencillos pero útiles puede ser lo decisivo a la hora de mantenerlos a salvo.



10 consejos importantes

1. Enseña a tus hijos a pararse a pensar antes de hacer clic en los enlaces y botones de descarga.
2. Enséñales a afrontar la comunicación online con precaución.
3. Configura las cuentas de tus hijos en modo privado.
4. Muéstrales que deben rechazar las solicitudes de amistad de extraños.
5. Mantén su sistema operativo y el software de seguridad actualizado.
6. Sé un buen modelo a seguir y mantén tu propio consumo digital bajo control.
7. Busca señales que puedan indicar que el niño es víctima de los ciberacosadores.
8. Utiliza una aplicación de control parental de confianza como ESET Parental Control.
9. Anímalos a utilizar contraseñas seguras.
10. Pídeles que piensen antes de compartir información personal, vídeos o fotos.