Guía para Padres

Sobre uso de Internet.

Pro@net

EL INTERNET DEL FUTURO

Introducción

Es posible que sus hijos pasen mucho tiempo en sitios web de mundos virtuales o de redes, populares representan un medio magnífico para interactuar con amigos mediante ordenadores y dispositivos móviles, y han cambiado la forma en que sus hijos se comunican con sus amigos y familiares.

Sin embargo, con mucha frecuencia los niños proporcionan demasiada información personal, comentan actitudes inapropiadas que podrían causarles problemas o se exponen de otras maneras al peligro debido a lo que comparten en Internet.

El objetivo de esta guía electrónica es ofrecer a los padres que están preocupados como usted el conocimiento necesario para enfrentarse a los desafíos relacionados con los sitios web de comunidades o de redes sociales.

Una vez que comprenda los principios básicos, será capaz de ayudar en mayor medida a sus hijos para que estén seguros en el momento de socializar
en Internet.

Porqué las redes sociales pueden ser peligrosas

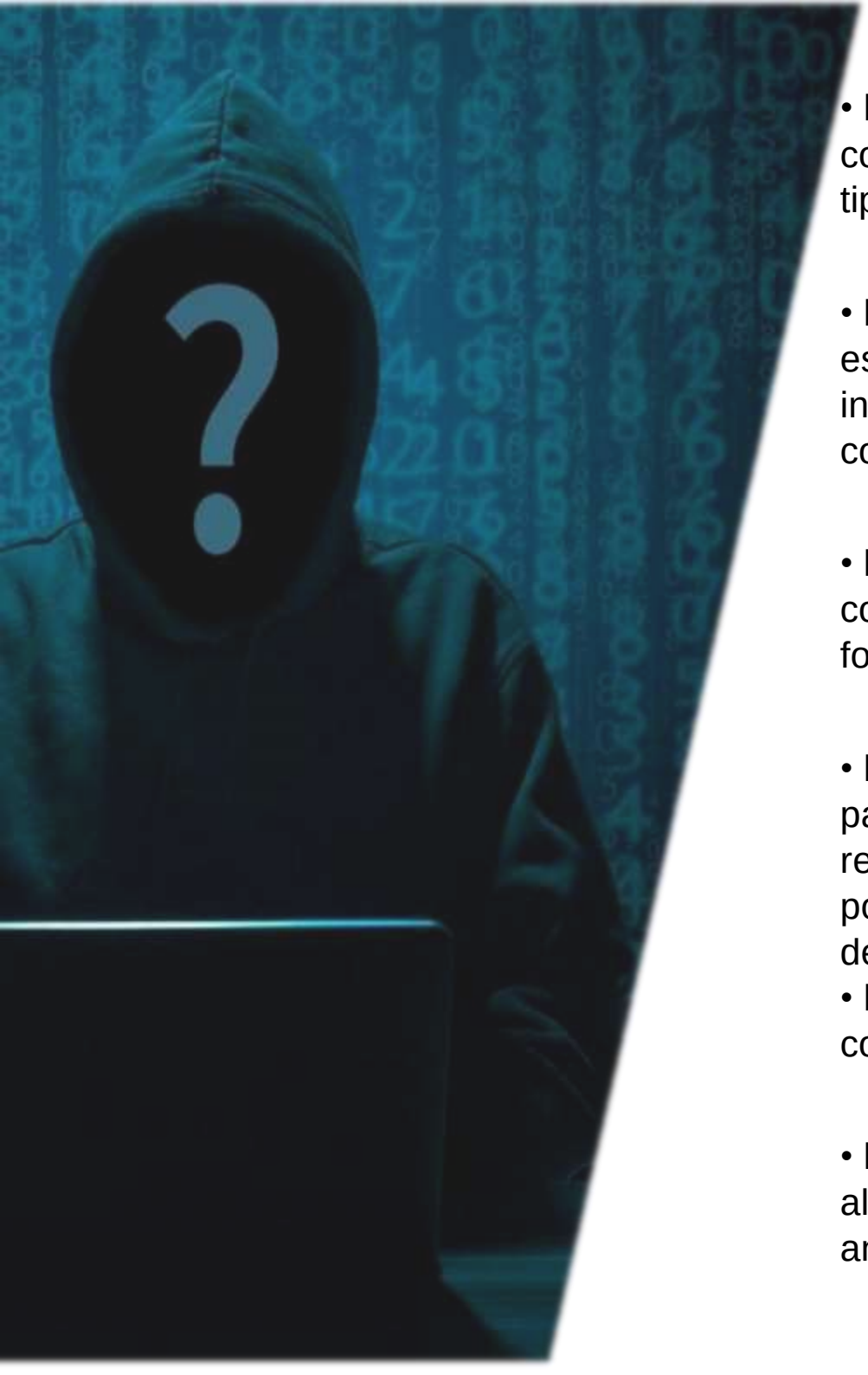
Quizá el mayor problema con las redes sociales pueda resumirse con las siglas “TMI” (del inglés too much information) o “demasiada información”.
Sus hijos deben comprender que si dan a conocer demasiados datos sobre su vida personal, esto podría causar problemas, como vulnerabilidad frente a los acosadores cibernéticos, los pederastas online, la invasión de la privacidad y el robo de identidad.
Estos problemas no se deben a las redes sociales, ya que han existido desde la llegada del correo electrónico y las charlas a través de Internet. Pero con las redes sociales, el volumen del contenido ha aumentado y se ha vuelto mucho más personal, y cualquier persona puede verlo con facilidad.
No sólo los niños corren peligro. Incluso los adultos se han visto avergonzados al colocar demasiada información en las páginas de sus perfiles a las que todo el mundo tiene acceso
Ejemplo de TMI en sitios web de redes sociales:
Se rechazó la admisión de un estudiante a una universidad debido a que elogió el lugar durante una visita al campus y luego la criticó duramente en Internet.

Hable con sus hijos y establezca límites

Los niños tienden a querer compartir información con sus amigos y contactos. Un perfil en un sitio web de red social es como una ventana hacia sus vidas. Deben comprender que necesitan proteger su privacidad y su reputación con diligencia.

Establezca algunos límites y cree algunas reglas para sus hijos con respecto a su comportamiento en Internet, especialmente en sitios de redes sociales.

- Limite la cantidad de tiempo que autoriza a sus hijos a estar conectados a Internet.
- Comente lo que es o no es apropiado para compartir online y recuerde a su hijo que no hay nada secreto en el ciberespacio.
- Aconseje a sus hijos que tengan cuidado con las personas que no conocen y que desean unirse a su red: estos “amigos” podrían ser pederastas o acosadores cibernéticos que quieren hacerles daño.



• Enséñeles los riesgos y peligros que implica el hecho de compartir contraseñas, números de teléfono, direcciones y otros tipos de información personal, incluso con sus mejores amigos.

• Recomiéndeles que no utilicen su nombre completo, ciudad, escuela y edad en ningún texto o imagen, de manera que esta información no pueda usarse para encontrarlos cuando no están conectados.

• Pídales que le comuniquen si notan algo extraño o inusual como, por ejemplo, mensajes de “amigos” que parecen atípicos o fotografías que sus hijos nunca publicaron.

• Enseñe a sus hijos a ser precavidos con los mensajes — en particular promociones u ofertas con vínculos a sitios web— que reciben de otras personas de su red, ya que los mensajes podrían provenir de un estafador que se ha apropiado del perfil de un amigo y está distribuyendo un “phishing”
• Explique a sus hijos que no pueden reunirse personalmente con individuos que hayan conocido online.

• Pida a sus hijos que confíen en sus instintos si sospechan de alguien: si alguna vez se sienten incómodos o amenazados, anímelos a que se lo comuniquen.

Acoso cibernético

El acoso cibernético es un problema que se plantea cuando sus hijos acceden a sitios de redes sociales.
* Dado que estos sitios se centran principalmente en compartir información personal, que se propaga con facilidad, no es difícil que sus hijos se conviertan en víctimas.
El acoso cibernético se define como el uso de Internet u otras tecnologías para enviar o publicar textos o imágenes con el propósito de perjudicar o avergonzar a otra persona.

Tipos de acoso cibernético:

• **Ataques en Internet:** peleas online que se envían por correo electrónico o mensajes instantáneos con lenguaje vulgar o con furia.
• **Hostigamiento:** enviar reiteradamente mensajes ofensivos, crueles u obscenos.
• **Difamación:** “faltar el respeto” a alguien online al enviar o publicar chismes o rumores acerca de una persona para dañar su reputación o sus amistades.

• **Suplantación:** fingir la identidad de otra persona y enviar o publicar material para dañar su reputación.

• **Bromas pesadas:** engañar a alguien para que revele información vergonzosa o secretos y luego distribuirlos online.

• Tiene mayor alcance: los mensajes de correo electrónico en que los niños se burlan de alguien pueden enviarse fácilmente a toda la clase o la escuela o, también, se puede publicar información en un sitio web accesible para todo el mundo.

• Puede ser anónimo.

• Tiene mayor alcance: los mensajes de correo electrónico en que los niños se burlan de alguien pueden enviarse fácilmente a toda la clase o la escuela o, también, se puede publicar información en un sitio web accesible para todo el mundo.

• Puede ser anónimo.

Esté atento a las señales de alarma y hable con sus hijos

Señales de alarma que indican que su hijo podría ser víctima de acoso cibernético

- Sentirse incómodo al recibir un mensaje de correo electrónico, instantáneo o de texto.
- Estar disgustado después de usar el ordenador.
- Negarse a salir de casa o a ir al colegio.
- Retraerse de amigos y familiares.
- Cambiar de pantalla o cerrar programas cuando usted se acerca.
- Usar el ordenador tarde por la noche.
- Enfadarse si no puede usar el ordenador.
- Utilizar varias cuentas en Internet o una cuenta que pertenezca a otra persona.

Si detecta alguna de estas señales, hable con sus hijos acerca de los problemas relacionados con el acoso cibernético, como víctimas y como autores. Anímelos a que no aprueben o apoyen a otros niños que ejercen acoso cibernético. Hágales preguntas basadas en las “señales de alarma” y luego siéntese a escuchar.

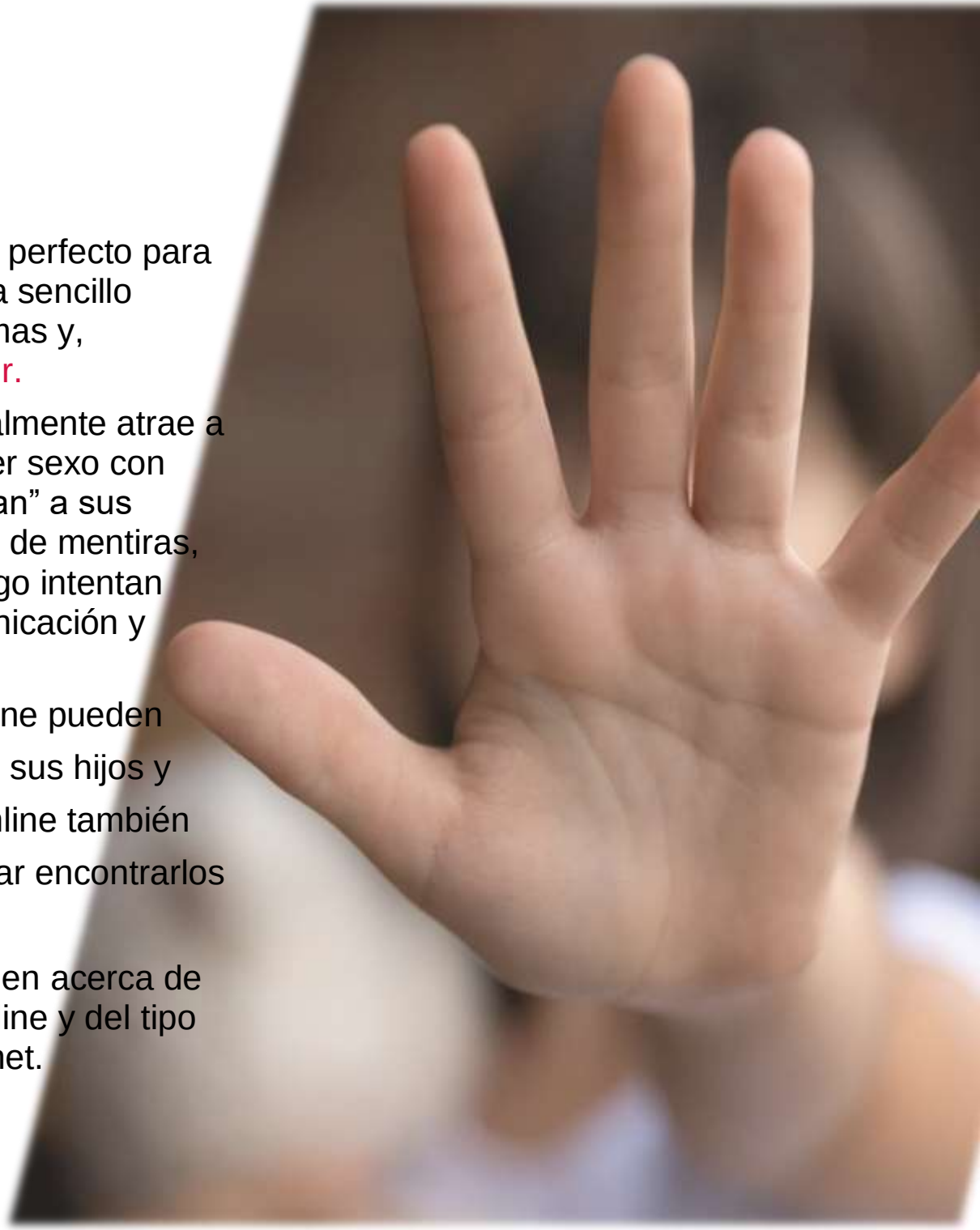
Pederastas online

Comúnmente se piensa que Internet es el entorno perfecto para los pederastas online considerando que les resulta sencillo ocultar su identidad, tener acceso a posibles víctimas y, además, hay un grupo enorme de niños para elegir.

Un pederasta online es un delincuente que generalmente atrae a los niños con el objetivo de manipularlos para tener sexo con ellos. Los pederastas online normalmente “preparan” a sus víctimas; generan confianza con el niño por medio de mentiras, extorsión y culpa, crean distintos personajes y luego intentan involucrar al niño en formas más íntimas de comunicación y posibles citas en persona.

En los sitios de redes sociales, los pederastas online pueden usar todas estas técnicas para hacerse amigos de sus hijos y tratar de involucrarse con ellos. Los pederastas online también usarán información del perfil de su hijo para intentar encontrarlos personalmente.

Por eso es fundamental que usted y sus hijos hablen acerca de los comportamientos apropiados cuando están online y del tipo de información que es aceptable publicar en Internet.



Anime a sus hijos a que informen sobre cualquier conducta inapropiada

Anime a sus hijos a que acudan a usted cuando los estén acosando en Internet o se hayan encontrado con algún pederasta online.

O, si no se sienten cómodos hablando con usted sobre estos temas, pídales que hablen con un adulto en quien confíen, una tía, un tío, un profesor o un hermano mayor, para hacerse escuchar

Asegúrese de que su hijo adolescente sepa cómo denunciar un abuso o comportamiento inapropiado en los sitios de redes sociales.

En Facebook, por ejemplo, pueden enviar un mensaje de correo

electrónico a abuse@facebook.com.

Invasión de la privacidad, suplantación maliciosa y robo de identidad

Si sus hijos no actúan con cuidado en los sitios de redes sociales, podrían convertirse en víctimas de invasión de la privacidad, suplantación maliciosa o robo de identidad.

La invasión de la privacidad puede darse con demasiada facilidad si sus hijos comparten sus contraseñas, si no son selectivos con las personas que añaden como amigos o no son cuidadosos con respecto a la información o las fotografías que publican online.

El nivel de visibilidad de las fotografías, perfiles o listas de amigos varía según el sitio; por lo tanto, sería prudente estar informado sobre las opciones de privacidad de los sitios que usan sus hijos. La clave para prevenir la invasión de la privacidad es asegurarse de que sus hijos sean cuidadosos con respecto a lo que comparten, con quién lo comparten y que comprendan que nada es privado cuando se publica en Internet, independientemente de la cantidad de controles que haya en el sitio Web.

La suplantación maliciosa se da cuando una persona finge ser su hijo y realiza actos maliciosos como publicar blasfemias o imágenes inapropiadas. La forma más sencilla de que alguien se haga pasar por su hijo es obtener su contraseña y, una vez que la tiene, puede publicar material inapropiado que parezca que proviene de su hijo.

La suplantación maliciosa también puede ocurrir cuando una persona finge ser alguien que no es en realidad e interactúa online con su hijo.

Una suplantación maliciosa de este tipo puede acarrear consecuencias fatales. Además, los pederastas online con frecuencia se hacen “amigos” de los adolescentes en Internet y los engañan presentándose como compañeros para atraer a sus víctimas y tener relaciones sexuales ilícitas.

El robo de identidad y phishing son cada vez más comunes en los sitios de redes sociales, en los que hay tanta información personal disponible para los hackers. Phishing se denomina a los intentos de engañar a las personas para que proporcionen información personal como contraseñas, números de teléfono y de tarjetas de crédito mediante promociones o peticiones falsas que parecen provenir de fuentes legítimas. Los ladrones de identidad que han conseguido las contraseñas de los miembros no sólo tienen acceso a sus perfiles, sino también a su red de amigos. Para los ladrones de identidad es muy sencillo utilizar las cuentas de las víctimas para enviar mensajes de phishing a una gran cantidad de personas, esperando que alguno de ellos caiga en su fraude y proporcione información confidencial.

Use la tecnología

• Utilice las opciones de configuración de seguridad y privacidad de los sitios de las redes sociales, tales como los perfiles privados, el bloqueo y la aprobación previa de comentarios para controlar con quién se comunican sus hijos.

• Asegúrese de tener el software de seguridad actualizado para su ordenador, que proteja al equipo de software malicioso, virus, spyware y otras amenazas.

• Contemple la posibilidad de usar un programa que le permita supervisar las actividades online de sus hijos y le ayude a protegerlos.

Qué hacer si su hijo se convierte en una víctima en Internet

Si su hijo se convierte en una víctima de un acechador cibernético o de un pederasta online, éstos son algunos de los pasos a seguir:

1. Tome medidas de inmediato

• Ignore el contacto por parte del acosador o pederasta online o no se conecte al sitio donde se produjo.

• Si el problema continúa, ignore el contacto por parte del acosador o pederasta online o no se conecte al sitio donde se produjo.

• Bloquee el nombre de pantalla y la dirección de correo electrónico del agresor, de manera que no pueda comunicarse con su hijo.

• Modifique la información que aparece en Internet sobre su hijo o, si es necesario, borre la cuenta.

• Póngase en contacto con el sitio donde se produjo el problema para pedir que eliminen la información y para denunciar al autor del acoso.

• Denuncie esto a su proveedor de servicios de Internet (ISP)
y al ISP del agresor.

2. Denuncie el incidente a las autoridades

3. Guarde las pruebas

• Conserve un registro de todas las comunicaciones del autor del acoso.

• Conozca el nombre de pantalla, la dirección de correo electrónico y el ISP del agresor, si tal información se encuentra disponible.

4. Aprenda todo lo que pueda acerca del uso que su hijo hace de Internet

• Averigüe qué servicios utiliza y qué le gusta hacer cuando está conectado.

• Infórmese sobre las funciones de seguridad de esos sitios web.

• Hable con su hijo acerca de la protección y la seguridad al conectarse a Internet.

Fuente:
https://www.mcafee.com/es-es/index.html