NET CÉTERA

Cómo charlar con sus hijos sobre su comportamiento en línea

TABLA DE CONTENIDOS

INTRODUCCIÓN

El internet ofrece un mundo de oportunidades.

Personas de todas las edades están:

- cargando videos desde aparatos portátiles
- creando perfiles en línea
- intercambiando mensajes de texto desde sus aparatos portátiles
- creando alter egos en línea por medio de avatares
- conectándose en línea con amigos que no ven en persona con regularidad
- difundiendo lo que están haciendo a cientos de personas

Estas formas de socializar y comunicarse pueden ser convenientes y agradables, pero vienen acompañadas de riesgos, algunos son:

Conducta inapropiada.

El mundo en línea puede dar la sensación de anonimato. A veces los niños se olvidan que continúan siendo responsables de sus acciones.

Contacto inapropiado.

En línea hay algunos individuos con malas intenciones, entre los que se incluyen los acosadores, intimidadores, depredadores, *hackers* y estafadores.

Contenido inapropiado.

Puede que esté preocupado por los contenidos pornográficos y violentos, el lenguaje obsceno o los insultos que sus hijos pueden encontrar en línea.

Usted puede reducir estos riesgos hablando con sus hijos sobre la manera en que se comunican—en línea y fuera de línea—y alentándolos a actuar de una manera que los enorgullezca.

Esta guía cubre lo que usted necesita saber, dónde recurrir para consultar más información y temas de conversación para tratar con sus hijos sobre cómo vivir sus vidas en línea.

¿Cuál es la mejor manera de proteger a sus hijos mientras están en línea?

Hablando con ellos.

Los investigadores indican que cuando los niños quieren obtener información importante, la mayoría de ellos confía en sus padres.

¿Tiene dudas sobre cómo empezar la conversación?

Considere lo siguiente:

Comience a temprana edad.

Después de todo, incluso los niños que recién comienzan a caminar ven que sus padres utilizan todo tipo de aparatos. Tan pronto como su hijo comience a usar una computadora, un teléfono celular o cualquier aparato móvil o portátil, es el momento indicado para hablar con él sobre cómo comportarse cuando está en línea y sobre la protección y la seguridad. Como padre, usted tiene la oportunidad de hablar con su hijo sobre estas cuestiones importantes antes de que lo haga otra persona.

Cree un ambiente sincero y abierto.

Los niños observan a sus padres como sus propios guías. Sea comprensivo y positivo. Escucharlos y tomar en cuenta sus sentimientos los ayuda a mantenerse atentos a la conversación. Es posible que usted no tenga todas las respuestas, y admitirlo sinceramente puede ser de gran ayuda.

Inicie la conversación.

Aunque sus niños se acerquen espontáneamente para hablar con usted, no espere a que sean ellos los que inicien la conversación. Aproveche las oportunidades que se presentan a diario para hablar con sus hijos sobre cómo actuar cuando están en línea. Por ejemplo, un programa de TV en el que aparece un adolescente navegando en línea o usando un teléfono celular puede presentar una oportunidad para hablar sobre qué es lo que se debe—o no se debe—hacer en una circunstancia similar. Por ejemplo, las noticias sobre estafas en internet, casos de ciber-acoso o ciber-violencia, también pueden servir para

comenzar una conversación con los chicos sobre sus experiencias y sus propias expectativas.

Comunique sus valores.

Sea directo sobre sus valores y de qué manera se aplican dentro del contexto en línea. Comunicar sus valores de manera clara puede ayudar a sus hijos a tomar decisiones más inteligentes y meditadas cuando se enfrentan a situaciones delicadas.

Tenga paciencia.

Resista las ganas de forzar la conversación con sus hijos. La mayoría de los chicos necesita que se le repita la información, en pequeñas dosis, hasta que logran incorporarla. Si sigue hablando con sus hijos, se verá recompensado a largo plazo por su paciencia y persistencia. Haga un esfuerzo para mantener abiertas las líneas de comunicación, incluso cuando sepa que su hijo hizo algo en línea que usted juzga inapropiado.

CONSEJOS PARA PADRES DE NIÑOS DE DIFERENTES EDADES

- Niños pequeños
- Preadolescentes
- Adolescentes

Niños pequeños

Cuando los niños pequeños comienzan a usar una computadora, deben estar supervisados de cerca por un padre o por la persona a cargo de su cuidado. Desde el comienzo, es conveniente que los padres elijan los sitios Web que pueden visitar sus hijos—y que no los dejen navegar a otros sitios solos. Si no se supervisa a los niños pequeños mientras navegan en línea, estos podrían tropezar con sitios que pueden asustarlos o confundirlos.

Cuando usted piense que su chiquito ya está preparado para explorar por su propia cuenta, es importante que usted esté cerca cuando vaya de un sitio a otro. Puede que quiera restringirle el acceso a sitios que usted ya ha visitado y sabe que son apropiados para la edad—por lo menos en lo que se refiere a su valor educativo o de entretenimiento.

Preadolescentes

Durante la etapa preadolescente (*tweens*)—entre 8 y 12 años—los niños comienzan a explorar con más independencia, pero esto no significa que usted no quiera —o no necesite—estar a mano.

Es importante estar con ellos—o por lo menos cerca de ellos—cuando están en línea. Si tiene hijos preadolescentes, considere instalar la computadora en un lugar de la casa en el cual el niño esté cerca de usted o de otro adulto. De esta manera, pueden ser "independientes", pero no estarán solos.

Las funciones de control paterno—filtros o herramientas de monitoreo—pueden resultar efectivas para los más chicos de este grupo. Pero, hay muchos chicos de esta edad que ya tienen los conocimientos técnicos necesarios para encontrar una manera de esquivar los controles. Si hasta ahora los chicos no habían comenzado a navegar por internet para hacer las tareas de la escuela, es probable que sea el momento en que empiecen a hacerlo. También es el momento en el cual pueden descubrir recursos para sus pasatiempos favoritos y demás intereses. Muchos preadolescentes son adeptos a la búsqueda de información en línea. Con frecuencia, ésta es una tarea útil para el resto de la familia, pero siguen necesitando del consejo de un adulto que los ayude a entender cuáles son las fuentes confiables.

Cuando considere qué es lo que sus hijos preadolescentes pueden hacer y ver en internet, piense también cuánto tiempo pasan en línea. Considere la posibilidad de establecer límites para la frecuencia y duración de sus sesiones de navegación en internet.

Muchos preadolescentes son adeptos a la búsqueda de información en línea pero siguen necesitando del consejo de un adulto que los ayude a entender cuáles son las fuentes confiables.

Adolescentes

Los preadolescentes tienden a reflejar los valores de sus padres. Cuando comienzan la adolescencia, los jóvenes ya están formando sus propios valores y comienzan a adoptar los valores de sus pares. Al mismo tiempo, los adolescentes más grandes están madurando física, emocional e intelectualmente, y muchos de ellos están ansiosos por experimentar una mayor independencia de sus padres.

Los adolescentes tienen un mayor nivel de acceso a internet a través de sus teléfonos celulares, aparatos portátiles o desde las computadoras de sus amigos, y también tienen más tiempo disponible para ellos. Por lo tanto, no es realista pensar que usted puede estar en el mismo cuarto que sus hijos adolescentes mientras que están en línea. Es necesario que ellos sepan que usted u otro miembro de la familia puede entrar y salir de su cuarto en cualquier momento y preguntarles qué están haciendo en línea.

Con los adolescentes es importante enfatizar el concepto de credibilidad. Hasta los chicos más expertos en tecnología necesitan comprender que no todo lo que ven en internet es real, que en internet las personas pueden ser distintas de lo que aparentan ser, que la información o imágenes que comparten en línea pueden ser vistas por todas partes, y que una vez que colocan algo en línea es casi imposible “sacarlo”.

Como no se pueden ver las expresiones faciales, ni el lenguaje corporal u otras claves visuales en las que confiamos fuera de internet, los adolescentes pueden sentir que en línea tienen la libertad de hacer o decir cosas que no harían de otro modo. Recuérdeles que detrás de los nombres de pantalla, perfiles y avatares hay personas de carne y hueso con sentimientos reales.

Cuando hable con su hijo adolescente, establezca expectativas realísticas. Anticipe cuáles serán sus reacciones si descubre que ha hecho algo en línea que usted desaprueba. Si su hijo adolescente le confía que vio en línea algo feo o inapropiado, intente tratar el tema con él para evitar que vuelva a suceder. Como su hijo adolescente se convertirá pronto en un adulto, necesita saber cómo comportarse y cómo actuar con prudencia para usar la red de manera segura, sin correr riesgos y de acuerdo a los principios éticos de su familia.

¿Qué puede hacer usted?

Los adolescentes y preadolescentes socializan en línea a través de sitios de redes sociales, salas de chateo, mundos virtuales y *blogs*. Los chicos comparten fotos, videos, ideas y planes con amigos, con otras personas que comparten sus propios intereses, y en ocasiones, con el mundo entero.

La socialización en línea puede ayudar a los chicos a conectarse con amigos e incluso con sus familiares, pero es importante que usted ayude a sus hijos a navegar estos espacios de manera segura. Entre los peligros que acarrea la socialización en línea se pueden mencionar el hecho de compartir demasiada información, o exhibir fotos, videos o palabras que pueden dañar la reputación o herir los sentimientos de otra persona. Aplicar la lógica y sentido común del mundo real puede ser útil para minimizar las desventajas de la socialización en el mundo virtual.

Recuérdeles a sus hijos que las acciones que tomen en línea pueden tener repercusiones.

Las palabras que escriben en línea y las imágenes que suben a los sitios tienen consecuencias fuera de internet.

Explíqueles a sus hijos que solamente deben colocar en línea la información que usted y ellos deseen que sea vista por otras personas.

Aunque estén activadas las funciones de seguridad, muchas más personas de las que usted quiere que lo hagan pueden ver el perfil en línea de su hijo. Aliéntelos a reflexionar sobre el tipo de lenguaje que usan cuando están en línea

y a pensar dos veces antes de subir fotografías y videos a su página o alterar fotos subidas por otra persona. Los empleadores, encargados de admisiones de las universidades, entrenadores deportivos, maestros, y la policía pueden ver lo que su hijo coloca en internet.

Recuérdeles a sus hijos que una vez que colocan la información en línea, no la pueden quitar.

Aunque eliminen la información de un sitio Web, tendrán muy poco control sobre las antiguas versiones que queden registradas en las computadoras de otras personas que pueden ser circuladas en línea.

Utilice las funciones de privacidad para limitar quien puede acceder y colocar información en el perfil de su hijo.

Algunos sitios Web de redes sociales, salas de chateo y *blogs* ofrecen funciones de privacidad muy efectivas. Hable con sus hijos sobre estas funciones de privacidad y sus expectativas con respecto a quien debería estar permitido a ver sus perfiles.

Revise la lista de amigos de su hijo.

Probablemente desee limitar la lista de "amigos" en línea a aquellas personas que su hijo conoce realmente.

Hable con sus hijos sobre evitar conversaciones sexuales en línea.

Los resultados de las investigaciones demuestran que los adolescentes que no hablan de sexo con extraños tienen menos probabilidades de entrar en contacto con un acosador. De hecho, los investigadores han descubierto que generalmente los acosadores no se hacen pasar por niños o adolescentes, y que la mayoría de los adolescentes que son contactados por adultos desconocidos lo ven como algo que les da escalofrío. Los adolescentes deben ignorar o bloquear a este tipo de individuos sin dudarlo.

Entérese de lo que están haciendo sus hijos.

Familiarícese con los sitios de redes sociales que usan sus hijos para entender mejor sus actividades. Si usted está preocupado porque piensa que su hijo se está comportando riesgosamente cuando está en línea, puede explorar los sitios de redes sociales que frecuenta para ver qué tipo de información está colocando. ¿Se están haciendo pasar por otro? Intente buscar por el nombre o apodo de su hijo, escuela, pasatiempos favoritos, grado que cursa o área de residencia.

Dígales a sus hijos que si tienen alguna sospecha confíen en sus instintos.

Aliéntelos a que le cuenten si cuando están en línea se sienten amenazados por alguna persona o se sienten incómodos con algo que ven en la red. Puede ayudarlos a reportar sus inquietudes a la policía y al sitio de redes sociales. La mayoría de estos sitios incluyen enlaces para que los usuarios puedan reportar inmediatamente los comportamientos abusivos, sospechosos o inapropiados en línea.

Dígales a sus hijos que no finjan ser otra persona.

Explíqueles a sus hijos que es inapropiado crear sitios, páginas o subir material que aparenta pertenecer a otra persona, como por ejemplo un maestro, un compañero de clase o un personaje inventado.

Pídales que creen un nombre de pantalla seguro.

Aliente a sus hijos a pensar en la impresión que pueden causar los nombres de pantalla. Un buen nombre de pantalla no debería revelar demasiada información sobre la edad, el lugar de residencia o género del usuario. Por razones de seguridad, los nombres que sus hijos utilicen para el chat no deberían ser iguales a los de sus domicilios de correo electrónico.

Ayude a sus hijos a entender que información debería permanecer privada.

Explíqueles la importancia de no dar a conocer datos sobre sí mismos, sus familiares y amigos. El nombre completo, número de Seguro Social, domicilio, número de teléfono e información financiera familiar—como por ejemplo los números de las cuentas bancarias o de tarjeta de crédito—es información privada y debe seguir siéndolo.

SEXTING

Enviar o reenviar fotos, videos o mensajes de sexo explícito desde un teléfono móvil es una práctica conocida como *sexting*, que es la abreviatura de las palabras *sex* y *texting*. Dígales a sus hijos que no lo hagan. Además de poner en riesgo su reputación podrían estar infringiendo la ley. Cuando los adolescentes son concientes de las consecuencias hay menos probabilidades de que tomen la decisión equivocada.

CIBER-ACOSO

El ciber-acoso es el acoso o intimidación en línea. Puede producirse por medio de un mensaje electrónico, mensaje de texto, en un juego en línea, o a través de comentarios difundidos en un sitio de redes sociales. Podría involucrar rumores o imágenes colocadas en el perfil de alguna persona o difundidos para que otros los vean, o crear un grupo o página para excluir a una persona.

Hable con sus hijos sobre el acoso o intimidación. Dígales a sus hijos que no pueden esconderse detrás de las palabras que escriben y las imágenes que difunden. Los mensajes hirientes no solamente hacen sentir mal al destinatario sino también dan una mala impresión sobre quien los envía—y a veces puede resultar en el desprecio de los compañeros y castigo de las autoridades.

Pídales a sus hijos que le cuenten si ven un mensaje o imagen que circula en línea que los hace sentir amenazados u ofendidos. Si teme por la seguridad de su hijo, establezca contacto con la policía.

- **Lea los comentarios.** Con frecuencia, el ciber-acoso involucra comentarios malvados y dañinos. De vez en cuando revise la página de su hijo para ver con qué se encuentra.

- **No reaccione.** Si su hijo es blanco de un acosador cibernético, dígale que no responda a la provocación. Por lo general, los matones buscan la reacción de sus víctimas. En su lugar, aliente a su hijo a tomar medidas juntos para guardar la evidencia y a hablar con usted sobre el tema. Si persisten los actos de intimidación, muéstrele la prueba a las autoridades escolares o las fuerzas del orden locales.

- **Proteja sus perfiles.** Si su hijo encuentra un perfil creado o alterado sin su permiso, contacte a la compañía que opera el sitio para que lo elimine.

- **Bloquee o elimine el nombre del acosador de la lista.** Si el acosador ejerce amenazas por medio de mensajes instantáneos u otro servicio en línea que tiene una lista de "amigos" o "compinches", elimine el nombre del acosador de las listas o bloquee su nombre de usuario o domicilio de correo electrónico.

- **Ayude a detener el ciber-acoso.** Si su hijo ve que alguna persona es víctima del ciber-acoso, aliéntelo a tratar de detenerlo evitando comprometerse o reenviando las amenazas y diciéndole al acosador que deje de hacerlo. Los investigadores dicen que por lo general, el acoso cesa bastante rápido

cuando intervienen los amigos de la víctima para defenderla. Una manera de ayudar a eliminar las prácticas de intimidación en línea es reportarlo al sitio o red donde las observa.

- **Reconozca los signos de un ciber-acosador.** ¿Podría su hijo ser el acosador? Busque indicios de comportamiento intimidatorio, como por ejemplo la creación de imágenes malvadas de otro chico.

- **Tenga presente que usted es un modelo para su hijo.** Los chicos aprenden a copiar a los adultos que difunden rumores o que se comportan con descortesía.

El correo electrónico, *chat*, IM, video llamadas y mensajes de texto son formas rápidas y convenientes de comunicarse.

Pero lo básico—qué decimos, cuándo lo decimos y por qué lo decimos—son iguales en línea y fuera de línea. La cortesía y el sentido común son partes importantes de toda comunicación, en cualquier lugar que se produzca.

¿Qué puede hacer usted?

Hable con sus hijos sobre sus modales en línea.

- **La cortesía y la buena educación son importantes.** Usted le enseña a sus hijos a ser educados en la vida real; hable con ellos sobre la importancia de comportarse educadamente también cuando están en línea. El envío de mensajes de texto puede parecer rápido e impersonal, pero las palabras amables como “pls” y “ty” son de uso común en los mensajes de texto, para abreviar por favor y gracias.
- **Bajando el tono.** Escribir un mensaje en letras mayúsculas, una larga serie de signos de exclamación o en tipografía muy destacada equivale a gritar. La mayoría de las personas no aprecia el griterío.
- **Cc: y Responder a todos: con cuidado.** Sugiérales a sus hijos que resistan la tentación de enviar un mensaje a todos los contactos de su lista.

- **Evitar los mensajes o cartas en cadena.** En el mejor de los casos, la mayoría de las cartas o mensajes en cadena son una molestia y en el peor de los casos son estafas. Muchas de estas cartas o mensajes acarrean virus o programas espía. Pídales a sus hijos que no los abran ni los reenvíen.

Configure las preferencias de alto nivel de privacidad en las cuentas de IM y video llamadas de sus hijos.

La mayoría de los programas de IM permite que los padres controlen si las personas de la lista de contacto de sus hijos pueden o no ver sus estatus en IM, incluso si están o no en línea. En algunas cuentas de IM y correo electrónico los padres pueden determinar quién puede enviar mensajes a sus hijos, y pueden bloquear a aquellos no estén en la lista.

Pregúnteles a sus hijos con quiénes se comunican en línea.

De la misma manera que usted quiere saber quiénes son los amigos de sus hijos fuera de línea, es conveniente que sepa con quién hablan en línea.

Hable con sus hijos sobre la importancia de crear contraseñas sólidas para las cuentas de e-mail y la necesidad de proteger estas contraseñas.

Cuanto más extensa sea la contraseña, más difícil resultará descifrarla. La información personal, su nombre de usuario, palabras de uso común o letras adyacentes en el teclado no son contraseñas sólidas. Para proteger sus contraseñas, los chicos deben evitar compartirlas con terceros, incluso con sus amigos.

Recuérdeles a sus hijos que protejan la información personal.

Los números de Seguro Social, números de cuenta y contraseñas son algunos ejemplos de los datos que deben mantenerse en privado.

PHISHING

Phishing es el nombre utilizado en inglés para denominar una práctica fraudulenta que se produce en internet cuando los estafadores envían mensajes de correo electrónico, mensajes de aparición automática (*pop-up*) o mensajes de texto para engañar a las personas y sacarles información personal y financiera. Luego usan la información para cometer robo de identidad.

Vea cómo usted—y sus hijos—pueden evitar una estafa de *phishing*:

- **No responda** a los mensajes electrónicos, de texto o de aparición automática que soliciten información personal o financiera ni haga clic sobre los vínculos o enlaces incluidos en estos mensajes. Tampoco utilice la función copiar y pegar (*cut and paste*) para colocar el domicilio de un enlace en el navegador de internet. Por ejemplo, si quiere consultar una cuenta financiera, escriba el domicilio Web que figura en su resumen de cuenta.

- **No dé información personal** por teléfono en respuesta a un mensaje de texto. Algunos estafadores envían mensajes de texto que aparentan provenir de un negocio legítimo pidiéndole que llame a un número de teléfono para actualizar los datos de su cuenta o para acceder a un "reintegro". Si usted les facilita su información, la utilizarán para gastar en su nombre.

- **Tenga mucho cuidado** al abrir o descargar los documentos o archivos adjuntados a los mensajes electrónicos recibidos, sin tener en cuenta quien sea la persona u organización que los envía. Estos archivos pueden contener virus o programas espías que el remitente desconoce.

- **Use un programa de seguridad** y actualícelo regularmente.

- **Lea la correspondencia** que recibe; revise los resúmenes de sus tarjetas de crédito y cuentas bancarias tan pronto como los reciba para controlar que no le hayan imputado cargos no autorizados.

- **Reenvíe los mensajes electrónicos de *phishing* a spam@uce.gov**—y a la compañía, banco u organización invocada falsamente en el mensaje *phishing*. También puede reportar el e-mail *phishing* al *Anti-Phishing Working Group* enviándolo a **reportphishing@antiphishing.org**.

Haga participar a sus hijos de estas actividades para que puedan desarrollar buenos hábitos de seguridad en internet. Comparta con ellos "momentos educativos"—si recibe un mensaje *phishing*, muéstreselos a sus hijos para ayudarlos a comprender que los mensajes que aparecen en internet no siempre son lo que aparentan ser.

TELÉFONOS MÓVILES: SOCIALIZACIÓN Y COMUNICACIÓN EN MOVIMIENTO

Enséñeles a sus hijos a tener en cuenta la seguridad cuando usan un teléfono celular.

¿Cuál es la edad apropiada para que un chico tenga un teléfono móvil? Esto es algo que debe decidir usted y su familia. Considere la edad de su hijo, su personalidad y madurez y las circunstancias familiares. ¿Es lo suficientemente responsable para cumplir las reglas que usted o la escuela establezcan para el uso del teléfono?

Muchas de las aplicaciones en línea también están disponibles en los teléfonos móviles—redes sociales, *blogs*, carga de contenidos, uso compartido de contenidos multimedia y edición de video. Enséñeles a sus hijos a tener en cuenta la seguridad cuando usan un teléfono celular.

¿Qué puede hacer usted?

Dígales a sus hijos que si comparten fotos y videos por teléfono lo hagan con mucho cuidado.

La mayoría de los teléfonos móviles ahora vienen con cámaras de foto y video, lo cual facilita que los adolescentes fotografíen o graben cada momento y lo compartan desde cualquier parte. Estas herramientas pueden fomentar la creatividad y la diversión; pero también presentan problemas relacionados con la reputación y seguridad personal. Aliente a sus hijos a pensar sobre su privacidad y las de los demás antes de compartir fotos y videos vía teléfono celular. Es fácil subir fotos y videos en línea sin el conocimiento—y mucho menos la aprobación—del fotógrafo o de la persona fotografiada. Puede ser abochornante e incluso riesgoso. Es más fácil pensárselo bien antes de compartir contenidos que controlar los daños luego.

No tolere el uso del teléfono móvil para intimidar o acosar a otros.

Los teléfonos móviles pueden utilizarse para intimidar o acosar a otras personas. Hable con sus hijos y dígales que traten a los demás de la misma manera que quieren que los traten a ellos. Los buenos modales y los principios éticos que le ha enseñado también se aplican a sus comunicaciones telefónicas.

Tenga buen juicio con respeto a las redes sociales móviles.

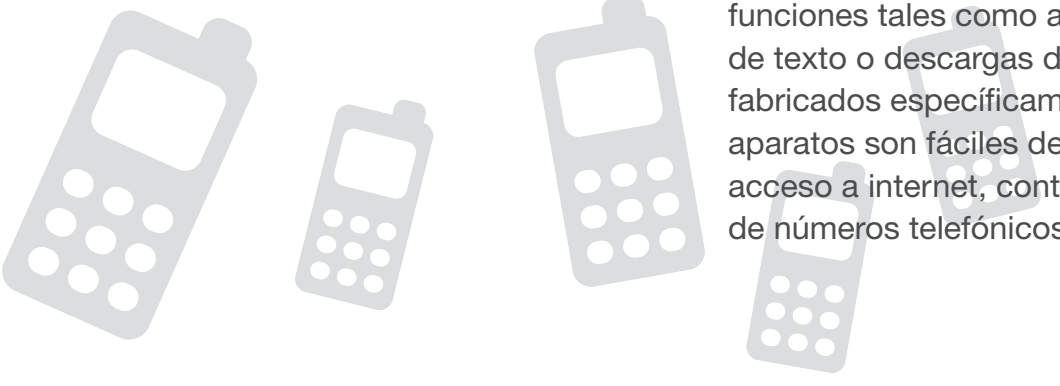
Muchos sitios de redes sociales permiten que los usuarios accedan desde sus teléfonos para revisar sus perfiles y colocar comentarios desde cualquier parte. Esto significa que los filtros que instaló en la computadora de su casa no limitarán las actividades de los chicos desde un teléfono. Si sus hijos adolescentes acceden a sus perfiles y a *blogs* desde sus teléfonos móviles, dígales que cuando lo hagan tengan buen juicio.

Familiarícese con el "mapeo" social.

Ahora, muchos teléfonos móviles vienen con tecnología GPS instalada: los chicos que tienen este tipo de teléfono pueden determinar con precisión dónde están sus amigos—y pueden ser localizados por sus amigos. Aconséjeles a sus hijos que usen estas funciones solamente con los amigos que conocen personalmente y en quienes confían, y explíqueles por qué no es bueno que difundan su ubicación a todo el mundo durante las 24 horas del día todos los días de la semana. Además, hay algunos proveedores que ofrecen servicios GPS para que los padres puedan determinar dónde se encuentran sus hijos.

Elija las opciones y funciones adecuadas del teléfono de su hijo.

La compañía de servicio de telefonía móvil y el teléfono deberían tener algunas opciones de control de privacidad y seguridad infantil. La mayoría de las compañías de servicio de telefonía móvil permiten que los padres desactiven algunas funciones tales como acceso a la red, mensajes de texto o descargas de archivos. Hay teléfonos fabricados específicamente para niños. Estos aparatos son fáciles de usar y tienen límites para el acceso a internet, control de minutos, privacidad de números telefónicos y botones de emergencia.



Sea inteligente con los teléfonos inteligentes.

Muchos teléfonos incluyen acceso a internet. Si sus hijos van a usar uno de estos teléfonos y a usted le preocupa qué es lo que pueden encontrar en la red, desactive el acceso a la red o active la función de filtro.

Establezca reglas para el uso del teléfono celular.

Hable con sus hijos sobre cuándo y cómo se debe usar el teléfono celular. También puede establecer reglas para su uso responsable. ¿Les permite recibir llamadas o intercambiar mensajes de texto a la hora de la cena? ¿Estableció reglas para usar el celular en la noche? ¿Deberían entregarle los teléfonos celulares mientras que hacen la tarea escolar para no distraerse, o cuando se supone que deberían estar durmiendo?

Dé el ejemplo.

Tener más aplicaciones en el teléfono móvil significa tener más elementos de distracción. En muchos estados es ilegal conducir mientras se envían o reciben mensajes de texto, mientras se navega la red o se habla por teléfono, pero hacerlo es peligroso en todos y cada uno de los estados. Dé el ejemplo y hable con sus hijos sobre el peligro que implica conducir distraído.

TEXTING

Probablemente, cualquier chico que tenga un teléfono celular lo use para enviar y recibir mensajes de texto e imágenes. Esto es similar al uso del e-mail o IM, y por lo tanto también se aplican la mayoría de las reglas de buena educación y seguridad. Si sus hijos intercambian mensajes de texto, aliéntelos a:

- respetar a los demás. Los textos abreviados pueden causar malentendidos. Antes de mandar un mensaje de texto hay que pensar cómo puede leerlo e interpretarlo quien lo reciba.
- ignorar los mensajes de texto enviados por desconocidos.
- aprender a bloquear números en su teléfono celular.
- evitar la difusión de su número de teléfono celular en línea.
- no dar nunca información financiera en respuesta a un mensaje de texto.

¿Qué puede hacer usted?

La seguridad de su computadora puede afectar su experiencia en línea—y también la de sus hijos. El *malware* es un software que monitorea o controla el uso de su computadora, puede instalar virus, o puede ser utilizado para enviar anuncios de aparición automática indeseados, redirigir su computadora a sitios Web que no desea visitar, o para grabar lo que escribe en su teclado. Si le instalan inadvertidamente un *malware* en su computadora, otra persona podría robarle la información personal de su familia.

Use un software de seguridad y actualícelo regularmente.

Los programas antivirus y *anti-spyware* escanean las comunicaciones entrantes para detectar los archivos problemáticos; el *firewall* bloquea las comunicaciones provenientes de fuentes no autorizadas. Busque programas con capacidad de revertir el daño y que se actualicen automáticamente.

Mantenga actualizados su sistema operativo y navegador de internet e infórmese sobre las funciones de seguridad.

Los *hackers* o piratas informáticos se aprovechan de los programas del sistema operativo y navegadores que no tienen instaladas las actualizaciones de seguridad más recientes. Aumente el nivel de seguridad de su computadora cambiando la configuración de seguridad y privacidad del sistema operativo o navegador de su computadora. Para aprender a cambiar la

configuración predeterminada de fábrica, consulte el menú de “Herramientas” (*Tools*) u “Opciones” (*Options*).

Tenga cuidado con las cosas “gratis.”

Los juegos, timbres de teléfono u otras descargas pueden esconder un programa malicioso o *malware*. Dígales a sus hijos que no descarguen nada a menos que confíen en la fuente y que lo hayan escaneado con el programa de seguridad.

P2P-ARCHIVOS COMPARTIDOS

Algunos chicos comparten música, juegos o programas en línea. El P2P o uso compartido de archivos es un sistema que permite que las personas compartan este tipo de archivos a través de una red informal de computadoras que utilizan el mismo programa. Si sus hijos descargan material protegido por la legislación de derecho de autor, usted podría verse involucrado en problemas legales. A veces, un archivo compartido puede tener escondido un programa espía, *malware* o material pornográfico. Le damos algunas recomendaciones para ayudar a sus hijos a compartir archivos sin riesgos:

- **Instale el software de archivos compartidos correctamente.** Active las características predeterminadas correctas para no compartir ninguno de los datos privados. Casi todas las aplicaciones de archivos compartidos o P2P vienen predeterminadas para compartir los archivos descargados en su archivo de “guardar” o “descargar”. Por esta razón, es importante configurar el programa para que no lo haga. Si usted no configura correctamente estas funciones, los demás usuarios de P2P pueden acceder a los archivos que usted no desea compartir, incluso a los documentos personales archivados en el disco duro de su computadora, como por ejemplo sus declaraciones de impuestos u otros documentos financieros.

- **Antes de que sus hijos abran o ejecuten un archivo descargado, dígales que lo escaneen con el programa de seguridad.** Asegúrese de que el programa de seguridad esté actualizado y en funcionamiento mientras que la computadora está conectada a internet.

CONTROLES PATERNOS

Si le preocupa lo que sus hijos pueden llegar a ver mientras navegan por internet—especialmente si tiene hijos en edad de escuela primaria—puede tomar en consideración algunas herramientas. Tenga presente que si bien los controles paternos pueden funcionar bien para los pequeños, los adolescentes que llevan años de experiencia en línea podrán desactivarlos o esquivarlos fácilmente o encontrar otras computadoras para acceder a los sitios que desean visitar.

Filtro y bloqueo.

Estas herramientas limitan el acceso a ciertos sitios, palabras o imágenes. Hay algunos productos que establecen por sí mismos qué material filtrar y hay otros que permiten que los padres establezcan los filtros. Algunos filtros se aplican a los sitios Web y hay otros que sirven para el e-mail, *chat* y mensajes instantáneos.

Bloqueo de contenido saliente.

Este software impide que los chicos compartan información personal en línea, en salas de chateo o vía e-mail.

Límite de tiempo.

Este programa le permite limitar la cantidad de tiempo que sus hijos pasan en línea y establece la hora del día en que pueden acceder a internet.

Navegadores para niños.

Estos navegadores filtran palabras o imágenes no aptas para el público infantil.

Motores de búsqueda para niños.

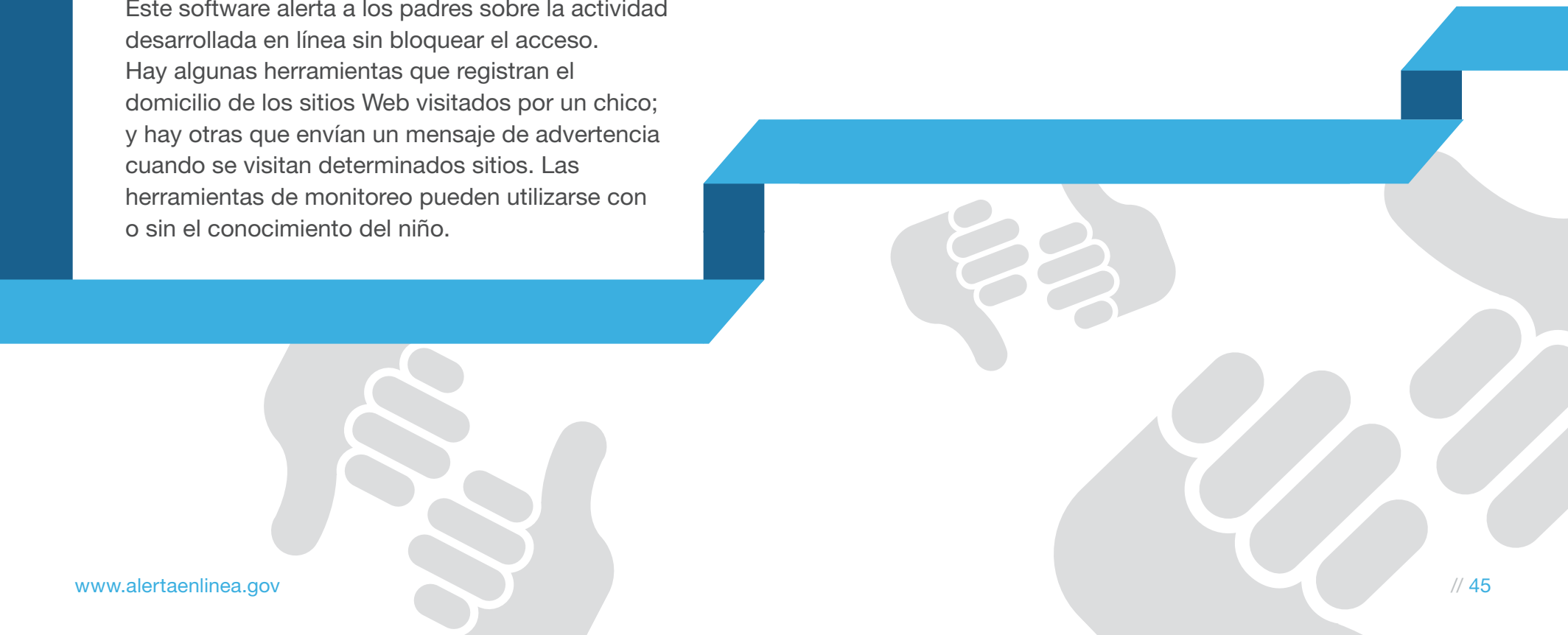
Estos motores hacen búsquedas limitadas o evalúan los resultados de la búsqueda de sitios y material apto para niños.

Herramientas de monitoreo.

Este software alerta a los padres sobre la actividad desarrollada en línea sin bloquear el acceso. Hay algunas herramientas que registran el domicilio de los sitios Web visitados por un chico; y hay otras que envían un mensaje de advertencia cuando se visitan determinados sitios. Las herramientas de monitoreo pueden utilizarse con o sin el conocimiento del niño.

La mejor manera de proteger a sus hijos mientras están en línea es hablar con ellos.

Cuando los niños quieren información importante, mayormente cuentan con sus padres. Los niños valoran las opiniones de otros niños. Pero tienden a confiar en sus padres para ayuda en los asuntos de mayor importancia.



PROTEJA LA PRIVACIDAD DE SUS HIJOS PREADOLESCENTES

La Ley de Protección de la Privacidad Infantil en internet (*Children's Online Privacy Protection Act*—COPPA) lo ayuda a proteger la privacidad de sus hijos otorgándole derechos específicos. La Comisión Federal de Comercio (*Federal Trade Commission*, FTC), la agencia nacional de protección del consumidor, está encargada de ejecutar y velar por el cumplimiento de la ley COPPA que exige a los sitios Web obtener el consentimiento paterno antes de recolectar o compartir información de menores de 13 años. La ley cubre a los sitios diseñados y dirigidos a menores de 13 años y aptos para todo público cuyos usuarios son sabidamente menores de 13 años. La ley COPPA protege la información recolectada por adelantado por los sitios Web y la información que sus hijos revelen o coloquen posteriormente.

La ley COPPA también establece que los sitios deben declarar su política de privacidad en un lugar visible y destacado. En el texto de la política de privacidad se debe informar detalladamente el tipo de información que recolectará el sitio y qué podrían hacer con dicha información—por ejemplo, si se prevé utilizar la información para enviar publicidad a sus hijos o para dársela a otras compañías. En la política de privacidad también se debe establecer si esas otras compañías han manifestado su acuerdo de mantener la información de manera segura y confidencial.

¿Qué puede hacer usted?

Aproveche los derechos que le otorga la ley COPPA. La información personal de su hijo es valiosa, y usted puede hacer muchas cosas para protegerla:

Sea selectivo con su permiso.

Los sitios pueden solicitarle su autorización por varios medios, entre los que se incluyen el correo electrónico o postal. Antes de dar su consentimiento asegúrese de saber qué información desea recolectar el sitio y qué es lo que prevé hacer con ella. También considere **qué grado de autorización** está dispuesto a conceder—en muchos casos no se trata de dar permiso para todo o nada. Posiblemente pueda dar autorización a la compañía para que recolecten algunos datos personales de su hijo, pero sin permitir que la compartan con terceros.

Sepa cuáles son sus derechos.

Como padre, usted tiene derecho a ver cualquier tipo de información personal que un sitio haya recolectado sobre su hijo. Si usted solicita ver la información, los operadores del sitio Web necesitarán comprobar que usted es realmente el padre o madre o pueden optar por eliminar la información. Usted también tiene derecho a revocar su autorización y exigir que eliminen la información sobre su hijo.

Controle los sitios Web que sus hijos visitan.

Si se trata de un sitio Web en el que los usuarios deben registrarse, vea qué tipo de información solicitan para hacerlo y evalúe si está o no de acuerdo con los datos que solicitan. También puede controlar si el sitio parece cumplir con las reglas más básicas, como por ejemplo exhibir la política de privacidad para padres de manera clara y destacada.

Lea la política de privacidad.

El sólo hecho de que un sitio tenga una política de privacidad no necesariamente significa que proteja la privacidad de la información personal. La política de privacidad puede ayudarlo a deducir si está de acuerdo con la información que recolecta el sitio y cómo prevé usar o compartir esa información. Si la política de privacidad dice que no limita la cantidad o tipo de datos que recolecta, o que no ejerce control sobre las personas que pueden acceder al sitio, significa que no hay límites.

Haga preguntas.

Si no entiende las prácticas o normas de un sitio Web, pida explicaciones. La política de privacidad debería incluir la información de contacto de una persona preparada para responder a sus preguntas.

Denuncie a los sitios Web que no cumplan las reglas.

Si cree que un sitio Web ha recolectado o divulgado información sobre sus hijos o que ha comercializado los datos de una manera contraria a la ley, presente una denuncia ante la FTC visitando **ftc.gov/queja**.

GLOSARIO

Asistente Personal Digital o PDA – "*Personal Digital Assistant*"—Aparato que puede utilizarse como teléfono móvil, navegador de internet o reproductor portátil de contenidos multimedia.

Avatar – Un alter ego gráfico creado por usted para utilizar en línea; puede ser un personaje en 3 dimensiones o un simple ícono, de aspecto humano o de fantasía.

Badware – Programa malicioso, incluye virus y programas espía para robar información personal, enviar *spam* y cometer fraude. (Ver programa malicioso.)

Blog – Abreviatura de "*web log*", un sitio donde usted coloca observaciones personales con regularidad.

Cámara Web—*Webcam* – Una cámara de video que puede emitir imágenes de video en vivo; puede estar incorporada a la computadora o puede comprarse por separado.

Ciber-acoso—*Cyberbullying* – Intimidación o acoso en línea; incluye subir fotos abochornantes o comentarios maliciosos al perfil de una persona o enviarlos vía mensaje instantáneo o e-mail.

Contraseña—*Password* – Una palabra o frase secreta utilizada junto a un nombre de usuario que le permite acceder a su computadora o proteger información delicada en línea.

Copias de seguridad—*Back up* – Hacer copias de los datos de su computadora le permite utilizarlas en caso de que le pase algo a su computadora o a su sistema operativo que cause la pérdida de la información.

COPPA – Ley de Protección de la Privacidad Infantil en internet (*Children's Online Privacy Protection Act*—COPPA) que le otorga a los padres el control sobre la información de los menores de 13 años que pueden recolectar los sitios Web.

Cuenta limitada de usuario—*Limited user account* – Una función en línea que da acceso a algunas de las funciones y programas de una computadora, pero solamente el administrador puede efectuar cambios que afecten la computadora.

Firewall – Hardware o software que bloquea las comunicaciones no autorizadas hacia o desde su computadora, ayuda a impedir que los hackers usen su computadora para enviar su información personal sin su autorización.

Funciones de privacidad—*Privacy settings* – Controles disponibles en muchos sitios de redes sociales y otros sitios Web que puede establecer para limitar las personas autorizadas a acceder a su perfil y a la información que pueden ver los visitantes.

Información personal—*Personal information* – Datos que pueden utilizarse para identificarlo, como por ejemplo su nombre, domicilio, fecha de nacimiento o número de Seguro Social.

Lista de amigos, lista de compinches—*Buddy list* – Una lista de personas con las que puede chatear a través de un programa de mensajes instantáneos (IM).

Mensaje Instantáneo, IM—*Instant Message* – Permite que dos o más personas conversen intercambiando mensajes en tiempo real y lo notifica cuando un amigo de su lista se encuentra en línea.

Mundo virtual—*Virtual World* – Un "lugar" en línea simulado por computación donde los usuarios usan avatares—personajes gráficos—para representarse a sí mismos.

Nombre de usuario—*User name* – Un alias utilizado junto con una contraseña para poder acceder a cuentas y sitios Web.

Parche—*Patch* – Software descargado para reparar o actualizar un programa de computación.

Perfil—*Profile* – Una página personal creada por usted en una red social u otro sitio Web para compartir información sobre usted y para comunicarse con otras personas.

Phishing – *Phishing* es el nombre utilizado en inglés para denominar una práctica fraudulenta que se produce en internet cuando los estafadores oportunistas envían mensajes de correo electrónico, mensajes de aparición automática (*pop-up*) o mensajes de texto para atraer con engaño a las personas y sacarles información personal y financiera u otros datos delicados.

Piratear—*Hacking* – Invadir una computadora o red evadiendo o desactivando las medidas de seguridad.

Preadolescente—*Tween* – Niño de entre 8 y 12 años de edad.

Programa de bloqueo—*Blocking software* – Un programa para filtrar el contenido de internet y restringir el acceso a sitios o contenidos sobre la base de un criterio específico.

Programa Espía—*Spyware* – Programa software instalado en su computadora sin su consentimiento para monitorear su uso o para controlar el uso de su computadora.

Programa malicioso—*Malware* – Abreviatura de "*malicious software*" incluye virus y programas espía para robar información personal, enviar spam y cometer fraude. (Ver *Badware*.)

Propiedad Intelectual—*Intellectual property* – Productos creativos que tienen valor comercial, incluye la propiedad protegida por los derechos de autor de libros, fotos, canciones, etc.

Sala de chateo—*Chat room* – Un espacio en línea donde usted puede encontrarse con otros usuarios e intercambiar información a través de mensajes que aparecen en las pantallas de otras personas que se encuentran en la "sala".

Sexting – Abreviatura de *sex* y *texting*. Enviar o reenviar fotos o mensajes con contenido de sexo explícito desde un teléfono móvil.

Sistema de Posicionamiento Global o GPS – Acrónimo de "*Global Positioning System*", un satélite de navegación global que se utiliza en automóviles o teléfonos para determinar la ubicación y dar instrucciones de orientación geográfica.

Sitio de redes sociales—*Social networking site* – Un sitio Web que le permite crear un perfil y conectarse con otras personas.

SMS – Abreviatura de *Short Messaging Service*; tecnología que permite enviar mensajes de texto desde un teléfono móvil a otro.

Software de seguridad—*Security software* – Programa de identificación y protección de amenazas o vulnerabilidades que pueden comprometer la seguridad de su computadora o su información personal; incluye programas antivirus y anti-spyware y firewall.

Teléfono inteligente—*Smart phone* – Un teléfono móvil que ofrece características avanzadas tales como conexión a internet y reproductor portátil de contenidos multimedia.

Texting – Intercambiar mensajes de texto cortos entre teléfonos móviles.

Uso Compartido de Archivos, P2P—*Peer-to-peer file-sharing* – Permite compartir archivos en línea—como música, películas o juegos—a través de una red informal de computadoras que operan el mismo software de uso compartido.

Video llamadas—*Video Calling* – Servicios de internet que permiten la comunicación entre usuarios por medio de cámaras Web.

Virus – Programa malicioso que se entromete inadvertidamente en su computadora—frecuentemente a través de un archivo adjuntado a un mensaje de correo electrónico—y que puede copiarse a sí mismo.

RECURSOS ADICIONALES

AlertaenLinea.gov – Recomendaciones prácticas brindadas por el gobierno federal y la industria tecnológica para ayudarlo a protegerse contra el fraude en internet, mantener su computadora segura y proteger su privicidad.

FTC.gov/robodeidentidad – Sitio Web de la Comisión Federal de Comercio que posee información para ayudarlo a detener, detectar y defenderse contra el robo de identidad.

GetNetWise.org – Un proyecto de *Internet Education Foundation*, la coalición GetNetWise desea que los usuarios de internet estén a "un clic" de los recursos necesarios para tomar decisiones informadas sobre el uso de internet personal y el de sus familias.

CyberBully411.org – Cyberbully411, creado por *Internet Solutions for Kids*, es un esfuerzo dirigido a brindar recursos para jóvenes que tienen preguntas sobre el acoso en línea o que han sido víctimas de ciber-intimidación.

ConnectSafely.org – ConnectSafely, es un proyecto de *Tech Parenting Group* para padres, adolescentes, educadores y personas interesadas en el tema para aprender sobre el uso seguro y civilizado de Web 2.0.

iKeepSafe.org – Los recursos educativos de iKeepSafe enseñan a los niños de todas las edades de manera divertida y acorde a la edad las reglas básicas de la seguridad, ética y el sano uso de las tecnologías de conexión.

NetFamilyNews.org – Es un nuevo servicio sin fines de lucro para padres, educadores y encargados de elaborar las políticas que desean mantenerse informados sobre las últimas novedades y comentarios tecnológicos sobre las actividades en línea de los jóvenes por medio de un blog diario o de boletines electrónicos semanales.

NetSmartz.org – NetSmartz Workshop es un recurso seguro interactivo y educativo del *National Center for Missing & Exploited Children* and *Boys & Girls Clubs of America* que emplea actividades en 3 dimensiones acordes a la edad para enseñar a los niños cómo mantenerse protegidos en internet.

WiredSafety.org – WiredSafety brinda ayuda, información y educación a los usuarios de internet y aparatos portátiles de todas las edades.

StaySafeOnline.org – A través de la colaboración con el gobierno, sectores empresariales, sin fines de lucro y académicos, la *National Cyber Security Alliance* procura crear una cultura de ciber-seguridad y concientización de seguridad brindando conocimientos y herramientas para prevenir el ciber-delito y los ataques informáticos.

Alerta en Línea

SU RED DE SEGURIDAD™

Alerta en Línea brinda recomendaciones prácticas del gobierno federal y la industria tecnológica para ayudarlo a protegerse contra el fraude en Internet, mantener su computadora segura y proteger su privacidad.

www.alertaenlinea.gov

Para ordenar copias gratuitas de este folleto, visite **bulkorder.ftc.gov**.