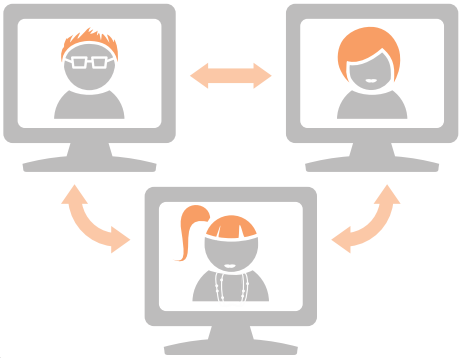
NETCÉTERA

Cómo charlar con sus hijos sobre su comportamiento en línea

Gente de todas las edades está:

Conectándose con amigos y familiares en internet



Descargando aplicaciones y accediendo a contenidos

Compartiendo lo que están haciendo — y donde están

Compartiendo fotos y videos desde aparatos móviles

Creando perfiles y reputaciones en línea

La comunicación en línea es un modo de vida, pero viene acompañada de ciertos riesgos:

- **Conducta inapropiada**
  El mundo en línea puede dar la sensación de anonimato. Los niños a veces se olvidan que continúan siendo responsables de sus acciones.

- **Contacto inapropiado**
  En línea hay alguna gente con malas intenciones. Uno podría encontrarse con acosadores, matones, depredadores, piratas informáticos y estafadores.

- **Contenido inapropiado**
  Es posible que usted esté preocupado por los contenidos pornográficos y violentos, el lenguaje obsceno o los insultos que sus hijos pueden encontrar en línea.

La tecnología está evolucionando constantemente. Y también los riesgos relacionados con la tecnología. Usted puede reducir estos riesgos hablando con sus hijos sobre cómo comunicarse — dentro y fuera de internet — y alentándolos a pensar con sentido crítico y actuar de una manera que los enorgullezca.

Esta guía de la Comisión Federal de Comercio cubre temas para tratar con sus hijos sobre viviendo la vida conectados.

HABLE CON SUS HIJOS

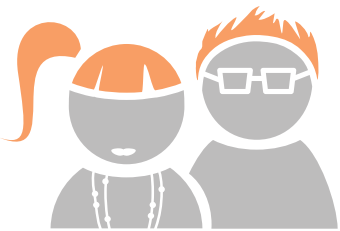
¿Cuál es la mejor manera de proteger a sus chicos mientras están en línea? Hablando con ellos. Aunque los chicos valoran las opiniones de sus pares, cuando necesitan ayuda para los asuntos de mayor importancia, la mayor parte de ellos tiende a confiar en sus padres.

Comience a temprana edad.

Los niños pequeños ven que sus padres usan todo tipo de aparatos — y también podrían verlos usando juegos o mirando programas en los aparatos. Tan pronto como su hijo comience a usar un teléfono, aparato móvil o una computadora, es el momento indicado para hablar con él sobre cómo debe comportarse y protegerse cuando está en línea.

Inicie las conversaciones.

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, una noticia sobre ciberacoso o sobre el envío de mensajes de texto mientras se conduce un vehículo puede ser un disparador para iniciar una conversación con sus hijos acerca de sus experiencias y sobre sus propias expectativas.



Comunique sus expectativas.

Sea franco sobre lo que usted espera de ellos y sobre cómo se aplican sus expectativas dentro del contexto en línea. Al comunicarles sus valores de manera clara usted puede ayudar a sus hijos a tomar decisiones más inteligentes y meditadas cuando se enfrenten a situaciones delicadas. Por ejemplo, explique específicamente qué es lo que está prohibido — y lo que usted considera un comportamiento inaceptable.

Tenga paciencia y sea comprensivo.

Resista las ganas de forzar la conversación con sus hijos. Para poder incorporar la información, casi todos los chicos necesitan que se la repitan en pequeñas dosis. Si sigue hablando con sus hijos, a la larga será recompensado 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.

Escucharlos y tener en cuenta sus sentimientos ayuda a mantener las conversaciones a flote. Tal vez usted no tenga todas las respuestas, y decirlo francamente puede ayudar mucho.

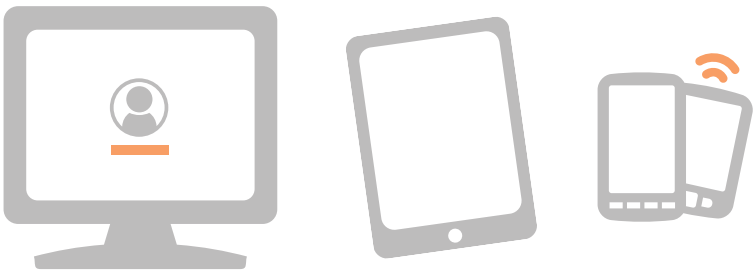
CONVERSACIONES PARA CADA EDAD

Niños pequeños

La supervisión es importante.

Cuando sus hijos pequeños comiencen a usar aparatos móviles o una computadora, deben ser supervisados de cerca por uno de sus padres o por la persona a cargo de su cuidado. Si los niños pequeños navegan en internet sin supervisión, podrían tropezar con contenidos que pueden asustarlos o confundirlos.

Cuando usted piense que su chiquito ya está preparado para explorar por su cuenta, es importante que siga estando cerca de él. Puede que quiera restringir el acceso para que su hijo pueda visitar sitios o aplicaciones que usted ya revisó y que considera que son apropiados para su edad — por lo menos en lo que se refiere a su valor educativo o de entretenimiento.



Considere usar los controles paternos.

Si le preocupa lo que sus hijos pueden ver en línea — considere usar herramientas con las siguientes funciones:

- **Filtro y bloqueo.** Estas herramientas limitan el acceso a ciertos sitios, palabras o imágenes. Hay algunos productos que establecen los filtros por sí solos y hay otros que permiten que los padres decidan qué material desean filtrar. Algunos filtros se aplican a los sitios web, y hay otros que sirven para el email y el chateo.
- **Bloqueo de contenido saliente.** Este software impide que los chicos compartan información personal en línea o vía email.
- **Límite de tiempo.** Este software le permite limitar la cantidad de tiempo que sus hijos pasan en línea y establecer la hora del día permitida para acceder a internet.
- **Navegadores para niños.** Estos navegadores filtran palabras o imágenes que usted no desea que vean sus chicos.
- **Motores de búsqueda para niños.** Estos motores hacen búsquedas restringidas o filtran los resultados de la búsqueda limitándolos a sitios y materiales aptos para niños.
- **Herramientas de monitoreo.** Este software alerta a los padres sobre la actividad 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 un niño visita determinados sitios. Las herramientas de monitoreo pueden utilizarse con o sin el conocimiento del niño.

Preadolescentes

Los chicos que están en la etapa preadolescente necesitan sentirse "independientes" pero no solos cuando comienzan a explorar por su cuenta. Muchos chicos de entre 8 y 12 años son adeptos a la búsqueda de información en línea, pero todavía siguen necesitando el consejo de un adulto que los ayude a entender cuáles son las fuentes confiables.

Piense en establecer ciertos límites.

Considere la posibilidad de establecer límites para la cantidad de tiempo y la frecuencia de sus actividades en línea — ya sea en la computadora, teléfono u otro aparato móvil. Los controles paternos pueden ser efectivos para los preadolescentes más chicos. Sin embargo, muchos niños en la escuela de enseñanza media (middle school, en inglés) tienen los conocimientos tecnológicos necesarios para sortear estos controles.

Adolescentes

Los adolescentes están formando sus propios valores y comenzado a adoptar los valores de sus pares. Muchos de ellos están ansiosos por experimentar una mayor independencia de sus padres. Sin embargo, necesitan aprender a ejercer su criterio y sentido común sobre la seguridad en línea y actuar de acuerdo a los valores éticos de sus familias.

Los adolescentes tienen un mayor nivel de acceso a internet a través de sus aparatos móviles — y también tienen más tiempo disponible para ellos. Por lo tanto, no es realista pensar que usted puede estar en el mismo cuarto mientras que están en línea. Es necesario que ellos sepan que usted u otro miembro de la familia puede preguntarles qué están haciendo en internet.

Hable sobre la credibilidad.

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.
- Es posible que la gente no sea lo que dice o aparenta ser en internet.
- La información o las imágenes que comparten en línea pueden ser vistas en todas partes.
- Una vez que suben o publican algo en línea, es casi imposible "quitarlo".

Hable sobre los buenos modales.

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

Hable sobre sus expectativas.

Cuando hable con sus hijos, establezca expectativas razonables. Prevea cómo va a reaccionar si descubre que sus hijos han hecho algo en línea que usted desaprueba.

Si su hijo le confía que vio algo feo o inapropiado mientras estaba en línea, intente hablar con él para ocuparse del tema y evitar que vuelva a suceder.

SOCIALIZACIÓN EN LÍNEA

Los chicos comparten fotos, videos, ideas, planes y el lugar donde están con sus amigos, familiares, y en ocasiones, con el mundo entero. La socialización en línea puede ayudar a los chicos a conectarse con otra gente, pero es importante que usted los ayude a navegar estos espacios sin riesgos.

Compartir demasiada información

Algunos de los peligros que acarrea la socialización en línea son compartir demasiada información, o el hecho de exhibir fotos, videos o palabras que pueden dañar la reputación de otra persona o herir sus sentimientos. Aplicar el criterio y sentido común del mundo real puede ser útil para minimizar estos inconvenientes.

¿QUÉ PUEDE HACER USTED?

Recuérdeles a sus hijos que sus acciones en internet tienen consecuencias.

Las palabras que los chicos escriben y las imágenes que suben tienen consecuencias fuera de internet.

- **Los chicos deberían publicar en internet solamente lo que deseen que los demás vean.** Aunque se usen funciones de privacidad, mucha más gente de la que usted — o ellos — desean pueden ver partes del perfil en línea de sus hijos. Aliente a sus hijos a reflexionar sobre el tipo de lenguaje que usan cuando están en línea y a pensárselo dos veces antes de subir fotografías y videos a su página o alterar fotos subidas por

otra persona. Los empleadores, encargados de admisión de las universidades, entrenadores deportivos, maestros, y la policía pueden ver lo que su hijo publica en internet.

- **Recuérdeles a sus hijos que una vez que publican algo en línea, no lo pueden quitar.** Aunque eliminen la información que publicaron en un sitio, tendrán muy poco control sobre las antiguas versiones que puedan quedar registradas en los aparatos de otra gente y que pueden seguir circulando en línea. ¿Y un mensaje que supuestamente se elimina del teléfono de un amigo? Hay programas que permiten guardarlo.

Dígales a sus chicos que limiten lo que comparten.

- **Ayúdelos a entender qué información debería permanecer privada.** Explíqueles la importancia de reservarse algunas cosas — sobre ellos, sus familiares y amigos — para sí mismos. Hay cierta información como el nombre completo, número de Seguro Social, domicilio y número de teléfono de los chicos y la información financiera familiar que es privada y debe seguir siéndolo.

- **Hable con sus hijos adolescentes sobre la importancia de evitar las conversaciones sexuales en línea.** Los adolescentes que no hablan de sexo con extraños cuando están en línea tienen menos probabilidades de entrar en contacto con depredadores sexuales. 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 contactados por adultos desconocidos lo sienten como algo que les da escalofrío. Los adolescentes deben ignorar o bloquear a este tipo de individuos sin dudarlo, y deben confiar en sus instintos cuando sientan que está sucediendo algo que les parece incorrecto.

- **Dígales que tengan cuidado con el envío de mensajes grupales.** Sugiérales a sus chicos que antes de enviar mensajes a varias personas piensen en quiénes necesitan verlos.

Limite el acceso a los perfiles de sus hijos.

- **Use las funciones de privacidad.** Muchos sitios de redes sociales, chateo y cuentas de video tienen funciones de privacidad ajustables, de modo que usted y sus chicos pueden limitar las personas que pueden ver los perfiles de sus hijos. Hable con sus chicos sobre la importancia de estas funciones y acerca de sus expectativas respecto de a quiénes se les debe permitir el acceso a sus perfiles.

- **Revise la lista de amigos de su hijo.** Sugiérales a sus hijos que restrinjan la lista de "amigos" en línea limitándola a aquellas personas que realmente conocen. Pregúnteles con quiénes están hablando en internet.

Ciberacoso

El ciberacoso es el acoso o intimidación en línea. Puede producirse por medio de un email, mensaje de texto, en un juego en línea, o en un sitio de redes sociales. Podría involucrar rumores o imágenes subidos al perfil de alguna persona o circulados para que otros los vean.

Ayude a prevenir el ciberacoso.

- **Hable con sus hijos sobre el acoso.** Dígales a sus hijos que no pueden esconderse detrás de las palabras que escriben y las imágenes que difunden o envían. El acoso es una situación en la que todos pierden: Los mensajes hirientes no solamente hacen sentir mal al destinatario sino que también dan una mala impresión sobre quien los envía. A menudo puede causar el desprecio de los compañeros y el castigo de las autoridades.

- **Dígales a sus hijos que también hablen con usted sobre el acoso.** Pídales a sus hijos que le cuenten si ven un mensaje o imagen que circula en línea que los hace sentir amenazados u ofendidos.

- **Reconozca los indicios de un ciberacosador.** Por lo general, el ciberacoso involucra comentarios malvados o malintencionados. Revise la página de red social de su hijo de vez en cuando para ver con qué se encuentra.

  ¿Podría ser su hijo el acosador? Busque indicios de comportamiento intimidatorio, como por ejemplo la creación de imágenes malvadas de otro chico.

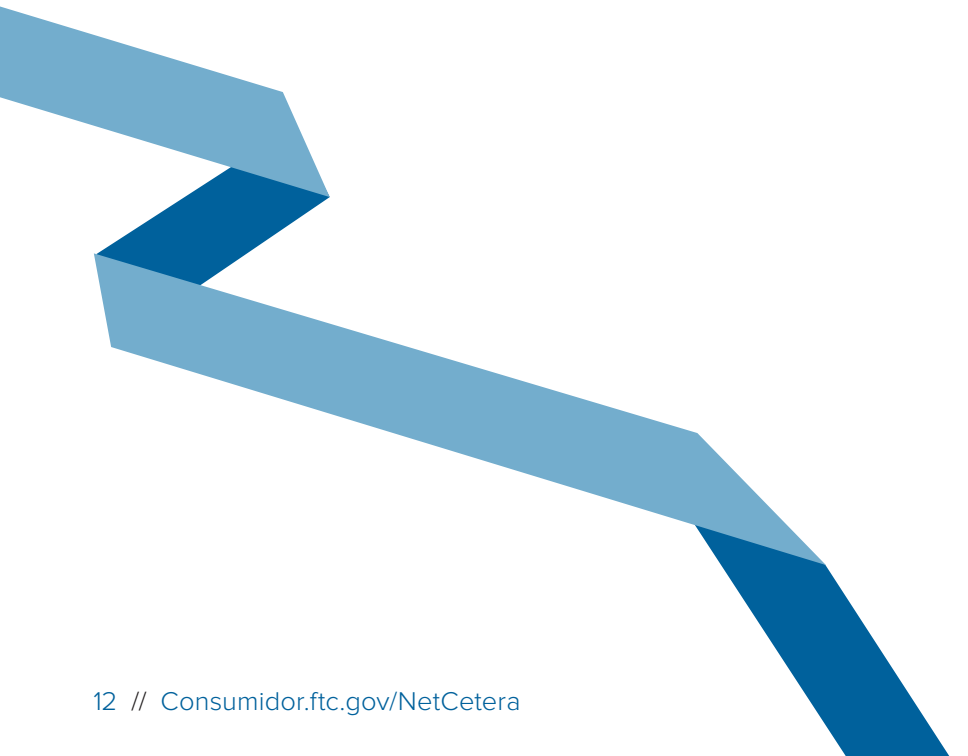
- **Ayude a detener el ciberacoso.** La mayoría de los chicos no acosan ni intimidan a otros y no hay ninguna razón para tolerar esta conducta. Aconséjeles a sus chicos que si ven que alguna persona es víctima del ciberacoso, traten de detener al acosador diciéndole que deje de hacerlo, y dígales que eviten involucrarse o reenviar alguna cosa amenazante. Una manera de ayudar a frenar el acoso en línea es reportar el incidente al sitio o red donde se lo observa.

Qué hacer ante un acosador.

- **No reaccione contra el acosador.** Si su hijo es blanco de un acosador cibernético, mantenga la cabeza fría. Recuérdele a su hijo que la mayoría de la gente sabe que está mal acosar a alguien. Dígale a su hijo que no responda de la misma manera. En su lugar, aliente a su hijo a enfrentar el tema con usted para guardar la evidencia y para que le hable sobre el asunto. Si persisten los actos de intimidación, muéstrele la prueba a las autoridades escolares o las fuerzas del orden locales.

- **Proteja el perfil de su hijo.** Si su hijo encuentra un perfil creado o alterado sin su permiso, comuníquese con el sitio para que lo elimine.

- **Bloquee o elimine al acosador.** Elimine al acosador de las listas de amigos o bloquee su nombre de usuario, domicilio de email y número de teléfono.



USO DE APARATOS MÓVILES

¿Cuál es la edad apropiada para que un chico tenga un teléfono o aparato móvil? Esto es algo que debe decidir usted y su familia. Considere la edad, personalidad y madurez de su hijo y las circunstancias familiares.

¿QUÉ PUEDE HACER USTED?

Teléfonos, funciones y opciones

Decida cuáles son las opciones y funciones correctas.

Su compañía de servicio de telefonía móvil y su teléfono deberían ofrecerle algunas opciones de control de privacidad y seguridad infantil. La mayoría de las compañías de telefonía móvil permiten que los padres desactiven algunas funciones tales como acceso a internet, mensajes de texto o descargas de archivos.

Hay teléfonos hechos especialmente para niños. Estos aparatos tienen un diseño fácil de usar y vienen con algunas funciones tales como acceso limitado 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 y aplicaciones móviles. Si sus hijos van a usar uno de estos teléfonos y a usted le preocupa lo que puedan encontrar en internet, escoja un teléfono con acceso limitado a internet o active la función de filtro web.

Familiarícese con los servicios de localización.

Hay muchos teléfonos móviles que vienen con tecnología GPS instalada. Los chicos que tienen este tipo de teléfonos pueden determinar con precisión dónde están sus amigos — y pueden ser localizados por sus amigos. Dígales a sus hijos que limiten estas funciones para que no estén difundiendo su ubicación a todo el mundo. Explíqueles que dejarle saber a todo el mundo dónde están puede causar inconvenientes. Además, hay algunos proveedores que ofrecen servicios GPS para que los padres puedan determinar dónde se encuentran sus hijos.

Proteja los teléfonos con contraseñas.

Para proteger un teléfono de los intrusos, se lo puede bloquear con una contraseña, código numérico o huella digital. Eso no solamente puede evitar que se marque un número accidentalmente, sino que también puede servir para impedir que la información y las fotos almacenadas en el teléfono caigan en las manos equivocadas.

Establezca reglas

Explique sus expectativas.

Hable con sus hijos sobre cuándo y cómo se debe usar el teléfono y otros aparatos móviles. También puede establecer reglas para que lo usen con responsabilidad. ¿Les permite recibir llamadas o intercambiar mensajes de texto, o jugar juegos en las aplicaciones a la hora de la cena? ¿Tiene alguna regla para usar el celular a la noche? ¿Deberían entregarle los teléfonos celulares mientras hacen la tarea escolar, o cuando se supone que deberían estar durmiendo?

Dé el ejemplo.

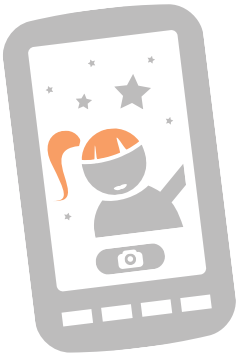
En la mayoría de los estados es ilegal manejar y textear o hablar por teléfono sin un accesorio de manos, pero hacerlo es peligroso en todos y cada uno de los estados. Dé el ejemplo a sus hijos, y hable con ellos sobre los peligros y consecuencias de conducir distraído.

Compartir contenidos y socializar

Socializar y compartir datos puede fomentar la creatividad y la diversión, pero al mismo tiempo podría causar problemas relacionados con la reputación y seguridad personal.

Compartir fotos y videos con cuidado.

La mayoría de los teléfonos móviles tiene cámara de fotos y de video, lo cual facilita que los adolescentes fotografíen o graben cada momento. Aliente a sus hijos a pedirle permiso al fotógrafo o a la persona fotografiada o filmada antes de subir videos o fotos. Es más fácil pensárselo bien antes de compartir contenidos que controlar los daños luego.



Tenga buen juicio cuando usa una red social móvil.

Los filtros que instaló en la computadora de su casa no servirán para limitar lo que puedan hacer los chicos desde un aparato móvil. Hable con sus hijos adolescentes sobre la importancia de usar el sentido común cuando socialicen desde sus teléfonos.

Aplicaciones móviles

¿Qué debería saber sobre las aplicaciones?

Las aplicaciones o apps podrían:

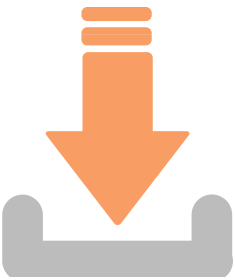
- Recolectar y compartir información personal.
- Permitir que sus hijos gasten dinero real — incluso cuando la aplicación es gratis.
- Incluir anuncios.
- Tener enlaces con medios sociales.

Pero puede que las aplicaciones no le digan que lo están haciendo.

¿QUÉ PUEDE HACER USTED?

Esto es lo que puede hacer usted junto a sus hijos para aprender más sobre la aplicación antes de descargarla:

- Mire las capturas de pantalla.
- Lea la descripción, la calificación del contenido y los comentarios de otros usuarios.
- Investigue un poco al desarrollador de la aplicación, lea particularmente las opiniones independientes de fuentes confiables.
- Fíjese en el tipo de información que recolecta la aplicación.



¿Puedo restringir la forma en que mis hijos usan las aplicaciones?

Antes de darles un teléfono o tablet a sus hijos, fíjese en la configuración del aparato. Es posible que pueda:

- **Restringir el contenido** limitándolo a aquello que considere apropiado a la edad de su hijo.
- **Establecer una contraseña** para que sus hijos no puedan descargar aplicaciones ni comprar nada sin ingresar la contraseña.
- **Desactivar la conexión WiFi y servicios de datos** o configurar el aparato en modo avión para que no se pueda conectar a internet.

La mejor manera de mantenerse al día sobre las aplicaciones para niños es probarlas por su cuenta y hablar con sus chicos sobre sus reglas para comprar y usar aplicaciones.

Textear

Aliente los buenos modales.

Si sus envían mensajes de texto, aliéntelos a respetar a los demás. Las abreviaciones que se usan en los mensajes de texto pueden generar malentendidos. Dígales que antes de enviar un mensaje de texto piensen cómo podría leerlo e interpretarlo quien lo reciba.

Proteja la privacidad.

Recuérdeles a sus chicos que:

- Ignoren los mensajes de texto enviados por desconocidos.
- Aprendan a bloquear números en sus teléfonos celulares.
- Eviten dar a conocer el número de su teléfono celular en línea.

Cómo reconocer un mensaje de texto spam.

Ayude a sus hijos a reconocer los mensajes de texto spam y explíqueles las consecuencias:

- A menudo contienen promesas de regalos gratuitos — o piden que se verifique la información de una cuenta — para lograr que se revele información personal.
- Pueden originar cargos no deseados en la factura de su teléfono celular.
- Pueden lentificar el funcionamiento del teléfono celular.

Fíjese si aparecen cargos no autorizados en la factura de su teléfono celular y repórtelos a su compañía de telefonía móvil. Dígales a sus hijos:

- **Que eliminen los mensajes que pidan información personal** — incluso cuando vienen con la promesa de un regalo gratis. Las compañías legítimas no piden información como números de cuenta ni contraseñas por email ni por mensaje de texto.
- **Que no respondan — ni hagan clic — en los enlaces del mensaje.** Los enlaces pueden instalar software malicioso y dirigirlos a sitios falsos que parecen reales pero que se establecen para robarle su información.

Sexteo

Enviar o reenviar fotos, videos o mensajes con contenido de sexo explícito desde un teléfono móvil es una práctica conocida como sexteo (sexting, en inglés). Dígales a sus hijos que no lo hagan. Si crean, reenvían o incluso almacenan este tipo de mensaje, además de poner en riesgo su reputación y sus amistades, también podrían estar infringiendo la ley. Cuando los adolescentes son conscientes de las consecuencias de sus actos, hay menos probabilidades de que tomen la decisión equivocada.

HACER UN HÁBITO DE LA SEGURIDAD INFORMÁTICA

La seguridad de su computadora, teléfono y otros aparatos móviles puede afectar la seguridad de su experiencia en línea — y la de sus hijos también. El software malicioso podría permitir que alguien robe la información personal o financiera de su familia. El software malicioso es un programa que puede:

- Instalar virus.
- Monitorear o controlar el uso de su computadora.
- Enviar anuncios de tipo *pop-up* indeseados.
- Redirigir su aparato a sitios web que usted no desea visitar.
- Registrar lo que escribe en su teclado.

¿QUÉ PUEDE HACER USTED?

- **Use un software de seguridad y manténgalo actualizado.** Las compañías reconocidas ofrecen muchas opciones gratuitas. Configure el software para que se actualice automáticamente.
- **Mantenga actualizados su sistema operativo y navegador de internet.** Los piratas informáticos se aprovechan de los programas que no tienen instaladas las actualizaciones de seguridad más recientes. También puede personalizar la configuración de seguridad y privacidad que viene instalada de fábrica en el sistema operativo o navegador de su computadora. Para explorar sus opciones vaya al menú de Herramientas u Opciones. Aproveche para actualizar sus aplicaciones al mismo tiempo.

Cómo enseñarles seguridad informática a los chicos

Hable con sus hijos sobre lo que pueden hacer para ayudar a proteger sus aparatos y la información personal de su familia.

Crear contraseñas sólidas y no compartirlas con nadie.

Cuanto más extensa es la contraseña, más difícil es descifrarla. La fecha de nacimiento, el nombre de usuario, o las palabras de uso común no son contraseñas seguras. Pídales a sus hijos que sean creativos y que creen contraseñas distintas para cada cuenta.

Puede ser tentador volver a usar la misma contraseña, pero si los piratas informáticos se la roban, podrán usarla para acceder a otras cuentas. Además, para proteger sus contraseñas, los chicos deben evitar compartirlas con otra gente, incluso con sus amigos.

No ingresar información personal o financiera a menos que el sitio web sea seguro.

Si usted o sus chicos envían mensajes, intercambian fotos, usan redes sociales o hacen trámites bancarios en internet, están enviando información personal a través de internet. Enséñeles a sus chicos que si la dirección de la página no comienza con **https**, no tienen que ingresar ningún dato personal. La letra “s” corresponde a seguro. Lo cual significa que la información que se está enviando está codificada y protegida.

Cuidado con las cosas “gratuitas”.

Los juegos, aplicaciones, archivos de música y otras descargas pueden esconder un software malicioso. No se debe descargar nada a menos que se confíe en la fuente. Enséñeles a sus hijos a reconocer las fuentes confiables.

Cuidado con los programas para compartir archivos.

Algunos chicos comparten música, juegos o programas en internet. Los programas para compartir archivos permiten que la gente comparta este tipo de archivos a través de una red informal de computadoras que utilizan el mismo programa.

A veces, en un archivo compartido se puede ocultar un programa espía, un software malicioso o material pornográfico. Si sus hijos descargan material protegido por la legislación de derecho de autor, usted podría verse involucrado en problemas legales. Es importante que hable con sus hijos sobre la seguridad y otros riesgos de los programas para compartir archivos.

- **Instalar correctamente el programa para compartir archivos.** Hay que revisar la configuración predeterminada para controlar que el programa no comparta ningún dato privado. Casi todas las aplicaciones para compartir archivos vienen predeterminadas para compartir los archivos descargados en su carpeta “Descargas” o “Compartido”.

  Si usted guarda sus archivos personales en las carpetas compartidas, otros usuarios del software para compartir archivos pueden acceder a los archivos que usted no desea compartir — incluso a documentos personales como sus declaraciones de impuestos u otros documentos financieros.

- **Usar un software de seguridad para escanear los archivos.** Antes que sus chicos abran o jueguen un archivo descargado, use un software de seguridad para escanearlo. Asegúrese de que el programa de seguridad esté actualizado y activado.

Cómo usar las conexiones WiFi públicas de manera segura

En muchos lugares públicos — cafeterías, bibliotecas y aeropuertos — se ofrecen puntos de acceso WiFi. Estos puntos de acceso a la red pueden ser convenientes, pero a menudo no son conexiones seguras. Lo cual podría facilitar que alguien acceda a las cuentas en línea de su familia o le robe su información personal — incluyendo documentos personales, fotos y contraseñas.

Usar redes WiFi seguras.

Las redes seguras usan un sistema de codificación que protege la información que se envía a través de internet cifrando los datos para que otras personas no puedan verlos ni acceder a ellos. Usted sólo puede estar seguro de que una red es segura si le pide que ingrese una contraseña **WPA** o **WPA2**.

Dígales a sus chicos que si la red no les pide una contraseña, no deberían usar esa red para conectarse a las cuentas ni para ingresar información personal. Y no hay que dar por supuesto que un punto de acceso WiFi codifica la información: la mayoría no lo hacen.

Usar sitios web seguros.

En un sitio web seguro su información será codificada mientras esté conectado — incluso si la red no la codifica. ¿Qué pueden hacer sus chicos para saber si es un sitio seguro? Dígales que busquen las letras **https** en la dirección web de cada página que visiten — no solamente en la página de inicio. La letra “s” corresponde a seguro.

No quedarse conectado permanentemente a las cuentas.

Recomiéndeles a sus chicos que se desconecten cuando terminen de usar un sitio.

Estafas de phishing

Phishing es el nombre utilizado en inglés para denominar una práctica fraudulenta que se produce cuando los estafadores oportunistas envían mensajes de texto, emails o mensajes emergentes para conseguir que la gente comparta su información personal y financiera. Los estafadores usan esta información para acceder a sus cuentas, robarle su identidad y cometer fraude.

¿QUÉ PUEDE HACER USTED?

Esto es lo que pueden hacer usted y sus chicos para evitar que los estafadores los engañen.

- **No responder a los mensajes de texto, emails, o mensajes emergentes que soliciten información personal o financiera**, ni hacer clic en los enlaces incluidos en los mensajes.
- **Tener cuidado al abrir o al descargar los archivos** adjuntados a los emails recibidos, cualquiera sea el remitente. Los archivos recibidos inesperadamente pueden contener virus que sus amigos o familiares desconocen.
- **Hacer participar a sus chicos** para que puedan desarrollar "antenas" para detectar estafas y desarrollar buenos hábitos de seguridad en internet. Comparta con ellos "momentos educativos" — si recibe un mensaje phishing, muéstreselos para ayudarlos a comprender que las cosas no siempre son lo que parecen.

Cómo reportar las estafas phishing.

Reenvíe los emails phishing a **spam@uce.gov**. Estos emails se agregarán a una base de datos utilizada por las agencias de cumplimiento de ley para iniciar investigaciones. Si usted o sus chicos fueron engañados con una estafa phishing, presente una queja en **ftc.gov/queja**.

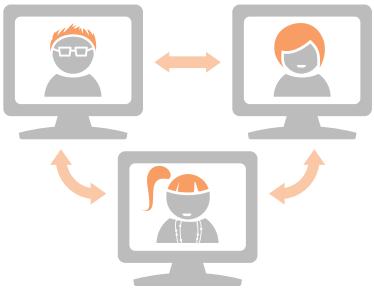
PROTEJA LA PRIVACIDAD DE SUS HIJOS

Como padre, usted tiene control sobre la información personal de sus hijos menores de 13 años que recolectan las compañías en internet. La Ley de Protección de la Privacidad Infantil en Internet (Children's Online Privacy Protection Act o COPPA, por su sigla en inglés) le da las herramientas para hacerlo.

La Comisión Federal de Comercio (FTC, por su sigla en inglés), ejecuta y vela por el cumplimiento de la ley COPPA. Si un sitio o servicio está cubierto por COPPA, debe obtener su consentimiento antes de recolectar la información personal de su hijo y debe respetar sus opciones de uso de esa información.

¿Qué es COPPA?

La ley COPPA fue implementada para proteger la información personal de los niños en los sitios web y servicios en línea — incluidas las aplicaciones — dirigidos a niños menores de 13 años. La ley también se aplica a sitios aptos para todo público que saben que están recolectando información personal de niños de esa edad.



Las disposiciones de COPPA establecen que esto sitios y servicios deben notificar a los padres directamente y que deben obtener su aprobación antes de recolectar, usar o revelar la información personal de un niño.

En el ámbito de COPPA la información personal de un niño incluye:

- Nombre.
- Domicilio.
- Número de teléfono o domicilio de email.
- Paradero físico.
- Fotos, videos y grabaciones de audio del niño.
- Identificadores persistentes, como domicilios IP, que puedan usarse para rastrear las actividades de un niño a lo largo del tiempo y a través de diferentes sitios web y servicios en línea.

¿Cómo funciona la ley COPPA?

Pongamos como ejemplo que su hijo quiere usar algo ofrecido por un sitio web o desea descargar una aplicación que recolecta su información personal. Antes de poder hacerlo, usted debería recibir un aviso redactado en lenguaje simple donde le digan qué información se recolecta, cómo se usa y cómo dar su consentimiento.

El aviso debe contener un enlace con una política de privacidad fácil de comprender. En la política de privacidad le deben dar detalles sobre el tipo de información recolectada por el sitio, y lo que podrían hacer con la información — por ejemplo, si prevén usar la información para enviarle publicidad a un niño, o si le darán o venderán esa información a otras compañías. Además, en la política le deberían indicar cómo comunicarse con una persona preparada para responder a sus preguntas.

Los sitios y servicios tienen cierta flexibilidad respecto del método para obtener su consentimiento. Por ejemplo, pueden pedirle que remita una nota de autorización proforma.

Otras pueden establecer un número de teléfono gratuito para que usted llame. Si usted acepta que el sitio o servicio recolecte información personal de su hijo, ese sitio o servicio tiene la obligación legal de almacenarla de manera segura.

¿Cuáles son sus opciones?

- **Comprenda las prácticas aplicables al manejo de la información del sitio.** Comience leyendo cómo prevé usar la información de su hijo esa compañía.
- **Sea exigente con su permiso.** Decida qué nivel de autorización desea dar. Por ejemplo, podría permitir que la compañía recolecte la información personal de su hijo, pero no permitir que compartan esa información con terceros.
- **Sepa cuáles son sus derechos.** Después de autorizar a un sitio o servicio para que recolecte información de su hijo, usted sigue teniendo el control. Como padre, usted tiene derecho a revisar la información personal recolectada sobre su hijo. Si usted pide ver la información, tenga presente que antes de permitirle acceder a los datos, los operadores del sitio web necesitarán comprobar que usted es realmente el padre o madre del niño. Usted también tiene derecho a revocar su autorización en cualquier momento y exigir que eliminen la información sobre su hijo.

¿Qué hacer si le parece que un sitio o servicio está incumpliendo las reglas?

Si cree que un sitio web ha recolectado información de sus hijos o ha comercializado los datos de una manera contraria a la ley, repórtelo a la FTC en **ftc.gov/queja**.

Consumidor.ftc.gov/NetCetera

Para obtener copias gratuitas de este folleto,
visite FTC.gov/ordenar.

PARA | PIENSA | CONÉCTATE®

Comisión Federal de Comercio // Enero 2014