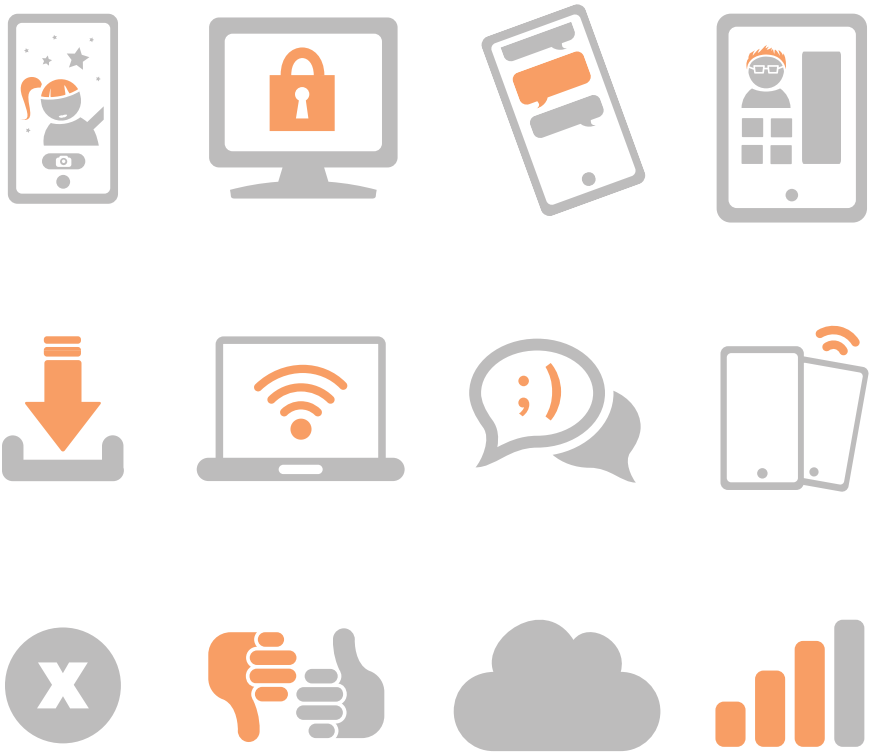
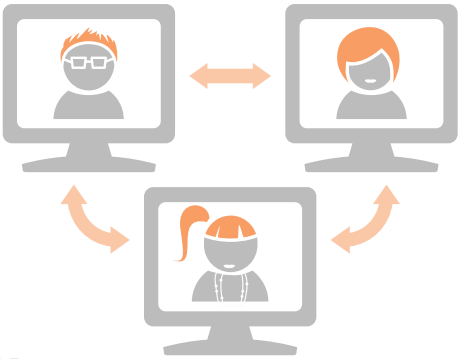
NETCÉTERA

Cómo charlar con los niños 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, depredadores, piratas informáticos o estafadores.
- **Contenido inapropiado**
  Es posible que usted esté preocupado por los contenidos pornográficos y violentos, el lenguaje agresivo u obsceno 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 chicos 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 (FTC) cubre temas para tratar con los niños sobre cómo vivir su vida mientras están conectados.

HABLE CON SUS HIJOS

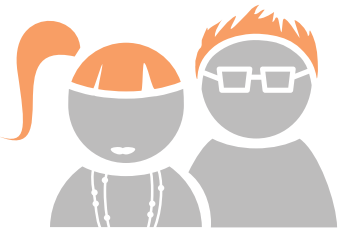
¿Cuál es la mejor manera de proteger a sus hijos mientras están en línea? Hablando con ellos. Aunque los niños valoran las opiniones de sus pares, la mayoría de ellos tiende a recurrir a sus padres cuando necesitan ayuda para los asuntos de mayor importancia.

Comience a edad temprana.

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 cuando su hijo comience 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 el ciberacoso o el intercambio 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 estas conversaciones con sus hijos. Para poder incorporar la información, la mayor parte de los niños necesita 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.

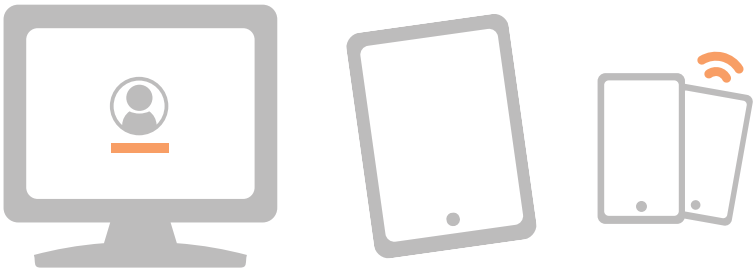
CONVERSACIONES PARA CADA EDAD

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 línea sin supervisión, podrían tropezar con contenidos que pueden asustarlos o confundirlos.

Cuando usted piense que su chiquillo ya está preparado para explorar por su cuenta, es importante que siga estando cerca. Puede que quiera restringir el acceso para que su hijo solo 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 ven en línea, considere usar herramientas con las siguientes funciones:

- **Filtro y bloqueo.** Estas herramientas limitan el acceso a ciertos sitios, aplicaciones, palabras o imágenes. Hay algunos productos que establecen los filtros por sí solos, y hay otros que permiten que los padres decidan lo que quieren filtrar.
- **Bloqueo de contenido saliente.** Este software impide que los chicos compartan información en línea o vía email.
- **Limitación 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 hijos.
- **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 tipo de 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 niño; 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.
- **Desactivación de las compras dentro de las aplicaciones desde su aparato.** Estas funciones pueden limitar o impedir que sus hijos hagan compras dentro de una aplicación desde su aparato.

Preadolescentes

Cuando los niños que están en la etapa preadolescente comienzan a explorar por su cuenta necesitan sentirse "independientes", pero no solos. Muchos niños 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 otros aparatos móviles. Los controles paternos pueden ser efectivos para los preadolescentes más pequeños. Sin embargo, muchos niños que están en la escuela de enseñanza media tienen los conocimientos tecnológicos necesarios para sortear estos controles.

Adolescentes

Los adolescentes están formando sus propios valores y comenzando 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 — de modo que no es realista pensar que usted pueda estar en el mismo cuarto con ellos 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 niños más expertos en tecnología necesitan comprender que:

- No todo lo que ven en internet es real
- La información o las imágenes que comparten en línea pueden ser vista en todas partes
- Es posible que la gente no sea lo que dice ser o aparenta ser en internet
- 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 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 que le dio miedo o que le pareció inapropiado mientras estaba en línea, intente hablar con él para ocuparse del tema y evitar que vuelva a suceder.

SOCIALIZACIÓN EN LÍNEA

Los niños comparten sus 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.

¿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 a la red 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 sus páginas 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 internet, no lo pueden quitar.** Aunque eliminen la información que publicaron en un sitio, tendrán muy poco control sobre las antiguas versiones que pudieran quedar registradas en los aparatos de otra gente y seguir circulando en línea. ¿Y un mensaje que se supone que se elimina del teléfono de un amigo? Hay aún algunas maneras de 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 sí mismos. Hay cierta información, como el número de Seguro Social, domicilio, número de teléfono e información financiera familiar que es privada y debe seguir siéndolo.

- **Hable con sus hijos adolescentes sobre la importancia de evitar 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 depredadores 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 escalofríos. Los adolescentes deben ignorar o bloquear a estos individuos, y deben confiar en sus instintos cuando sientan que está sucediendo algo que les parece incorrecto.

- **Dígales a los chicos que no solo se trata de lo que publican en línea.** Aunque no publiquen información, se la puede recolectar y compartir igual. Por ejemplo, los sitios web que visitan, la actividad en los medios sociales o las respuestas a cuestionarios se puede compartir o usar para fines de publicidad.

Limite el acceso a los perfiles de sus hijos.

- **Use las funciones de privacidad.** Muchos sitios de redes sociales, cuentas de chateo y de videos tienen funciones de privacidad ajustables, de modo que usted y sus hijos pueden limitar las personas que pueden acceder a los perfiles de sus hijos. Hable con sus hijos sobre la importancia de estas funciones y acerca de sus expectativas con respecto 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 la persona que los envía. A menudo pueden causar el desprecio de los compañeros y el castigo de las autoridades.

- **Reconozca los indicios de un ciberacosador.** Por lo general, el ciberacoso involucra comentarios malvados o malintencionados. Revise las páginas de redes sociales 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 niño.

- **Aliente a sus hijos a hablar en voz alta del tema.** Habitualmente, el ciberacoso se frena bastante rápido cuando alguien lo denuncia. Aconséjeles a sus hijos 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 comprometida. Si su hijo ve que un amigo está publicando algo grosero o desconsiderado, aliéntelo a hablar con ese amigo.

Otra 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 ciberacosador.

- **No reaccione contra el acosador.** Si su hijo es blanco de un acosador cibernético, mantenga la calma. 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 a 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 el nombre del 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 niño 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 móvil deberían ofrecerle 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. Usted también puede desactivar las compras dentro de las aplicaciones para que su hijo no pueda gastar un montón de dinero accidentalmente mientras juega a su juego favorito.

Sea inteligente con los teléfonos inteligentes.

Muchos teléfonos ofrecen acceso a internet y a aplicaciones móviles. Si sus hijos van a usar un teléfono 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 niños 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. Pero también hay servicios GPS (ofrecidos por algunos proveedores) que permiten que los padres puedan localizar a sus hijos.

Proteja los teléfonos con contraseñas.

Para proteger un teléfono de los intrusos, se lo puede bloquear con una contraseña, código numérico, control por gestos 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 es conveniente que establezca reglas para que los usen con responsabilidad. ¿Les permite recibir o hacer llamadas, intercambiar mensajes de texto o jugar con aplicaciones a la hora de la cena? ¿Tiene alguna regla para usar el celular a la noche? ¿Deberían entregarle los teléfonos a usted 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 un vehículo y textear o hablar por teléfono sin un accesorio de manos libres, pero hacerlo es peligroso en todas partes. Dé el ejemplo a sus hijos, y hable con ellos sobre los peligros y consecuencias de conducir distraído.

Compartir contenidos y socializar con aparatos móviles

Socializar y compartir datos desde cualquier lugar y en cualquier momento puede fomentar la creatividad, pero al mismo tiempo podría causar problemas relacionados con la reputación y la 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 antes de subir videos o fotos en internet. Es más fácil pensárselo bien antes de compartir contenidos que controlar los daños luego.

Ser prudente cuando se use una red social desde un aparato móvil.

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

Aplicaciones móviles

¿Qué debería saber sobre las aplicaciones?

Las aplicaciones, o apps, podrían:

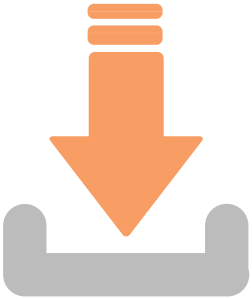
- recolectar y compartir información personal
- permitir que sus hijos gasten dinero real — incluso cuando la aplicación es gratis
- incluir anuncios
- tener enlaces con medios sociales

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 una aplicación antes de descargarla:

- mirar las capturas de pantalla
- leer la descripción, la calificación del contenido y los comentarios de otros usuarios
- investigar un poco al desarrollador de la aplicación y leer 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 lo que considere apropiado para 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 servicio de datos** o configurar el teléfono en modo avión para que no se puedan conectar a internet.

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

Textear

Aliente los buenos modales.

Si sus hijos usan 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 piensen cómo podría leerlo e interpretarlo quien lo reciba.

Proteja la privacidad.

Recuérdeles a sus hijos 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
- nunca den información personal ni financiera en respuesta a un mensaje de texto

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 su factura de 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 o contraseñas, por email ni por mensaje de texto.
- **Que no respondan — ni hagan clic — en los enlaces del mensaje.** Los enlaces pueden instalar programas maliciosos y dirigirlos a sitios falsos que parecen reales pero que se establecen con la intención de robarles su información.

Sexteo: No lo hagan

Enviar o reenviar fotos, videos o mensajes con contenido de sexo explícito desde un teléfono móvil es una práctica conocida como “sexteo”. Dígales a sus hijos que no lo hagan. Si crean, reenvían o incluso si almacenan este tipo de mensajes, 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

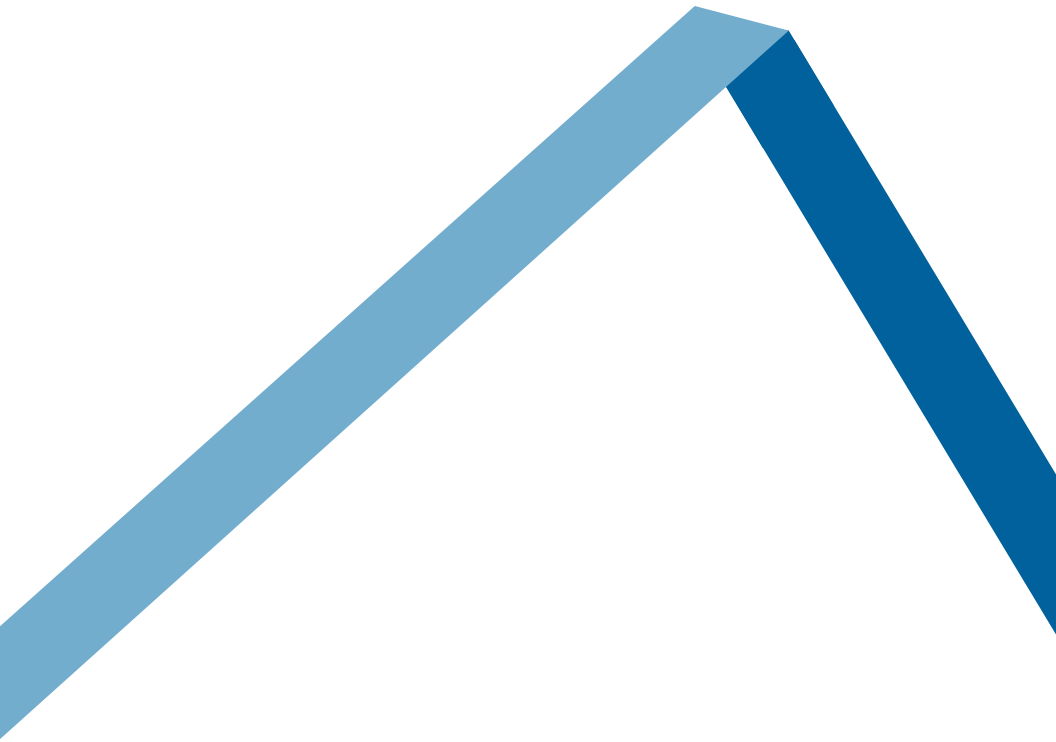
La seguridad de su computadora, teléfono y otros aparatos móviles puede afectar la seguridad de su experiencia en línea — y la de sus hijos. Un software o programa malicioso podría permitir que alguien robe la información personal o financiera de su familia. El software malicioso es un programa que puede:

- instalar un virus
- monitorear o controlar el uso de su computadora
- enviar anuncios de tipo pop-up indeseados
- redirigir su aparato a sitios web que no se desea visitar
- registrar lo que se escribe en el 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, el navegador de internet y las aplicaciones.** Los piratas informáticos se aprovechan de los programas que no tienen las actualizaciones de seguridad más recientes.
- **Si las cuentas de su familia están habilitadas para funcionar con el sistema de autentificación multi-factores, considere usar uno de estos sistemas.** El hecho de tener que usar su contraseña más otro dato para iniciar una sesión ayuda a proteger su cuenta, incluso si la contraseña queda expuesta. El segundo dato podría ser un código enviado a su teléfono, o un número aleatorio generado por una aplicación o token de seguridad.



Cómo enseñarles seguridad informática a los niños

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.

Fíjese en las contraseñas que usan usted y sus hijos. Para proteger mejor las cuentas, hay que crear contraseñas que tengan un mínimo de doce caracteres y que incluyan letras minúsculas y mayúsculas, números y símbolos. Evite usar palabras, frases o datos como su domicilio. Use contraseñas distintas para cuentas diferentes. De ese modo, si un pirata informático logra acceder a una cuenta, no podrá acceder a las otras.

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

Si usted o sus hijos envían mensajes, intercambian fotos, usan redes sociales o hacen trámites bancarios en línea, están enviando información personal a través de internet. Enséñeles a sus hijos que si la dirección de la página no comienza con **https**, no tienen que ingresar ningún dato personal. Esa “s” 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 gratis 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.

Haga copias de seguridad de sus archivos con regularidad.

No hay ningún sistema completamente seguro. Si usted o sus hijos tienen archivos importantes, cópielos en un disco externo o almacénelos en la nube. Si su computadora sufre un ataque de un programa maliciosos, aún podrá acceder a sus archivos.

Proteja la red de su casa.

Si en su casa usa internet sin cable, usted tiene una red inalámbrica. Al proteger esa red protegerá los aparatos de su familia contra los piratas informáticos y al mismo tiempo protegerá su información personal o financiera.
Estas son algunos pasos fáciles que puede seguir para proteger su red:

- **Active la codificación.** La codificación cifra la información que usted envía a través de internet en un código para que los demás no puedan acceder a ella. Esta es la forma más efectiva de proteger su red.

  Su computadora, enrutador y otros equipos deben usar la misma codificación. WPA2 es el sistema de codificación más potente; si tiene esta opción disponible, úsela.

- **Cambie la o las contraseñas predeterminadas de su enrutador.** Los piratas informáticos conocen las contraseñas predeterminadas, así que cámbielas por algo más complejo (ver recomendaciones para contraseñas en la página 24).
- **Mantenga actualizado su enrutador.** Al igual de lo que sucede con los otros aparatos, para que su enrutador sea seguro y efectivo, es necesario actualizarlo de tanto en tanto.

Cómo usar las conexiones WiFi públicas de manera segura

En muchos lugares públicos — como cafeterías, bibliotecas y aeropuertos — se ofrecen puntos de acceso Wi-Fi. 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.

¿QUÉ PUEDE HACER USTED?

No usar redes WiFi públicas para acceder a información financiera o personal.

Recuérdeles a sus hijos que la conexión WiFi no es segura. Eso significa que los otros usuarios que están conectados a esa red pueden ver lo mismo que uno está viendo o enviando. La información personal de su familia, los

documentos privados y las credenciales para los inicios de sesión en cuentas en línea, y otros datos podrían estar al alcance de la mano de otras personas.

¿Cuál es la solución más fácil? Establezca una regla para que todas las transacciones de compras, bancos y demás transacciones personales que haga su familia se hagan desde la red de su casa. Luego asegúrese de que la red de su casa esté codificada. Cuando esté fuera de su casa, use sus datos móviles — y dígales a sus hijos que hagan lo mismo.

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 hijos para saber si un sitio es seguro? Dígales que busquen las letras **https** en la dirección web de cada página que visiten — no solamente en la página de inicio de sesión.

No quedarse conectado permanentemente a las cuentas.

Recomiéndeles a sus hijos 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, o pop-up, 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 hijos para evitar que los estafadores oportunistas los engañen.

- **No responder a los mensajes de texto, emails o mensajes emergentes que soliciten información personal o financiera**, ni tampoco hacer clic en los enlaces incluidos en el mensaje.
- **Tener cuidado al abrir o descargar archivos adjuntos** o al descargar cualquier archivo adjuntado 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.

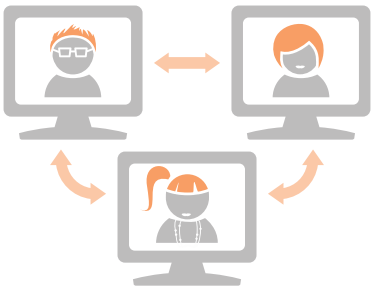
Cómo reportar las estafas de phishing

Reenvíe los emails phishing a **Spam@uce.gov**. Estos emails se agregarán a una base de datos utilizada por las agencias a cargo del cumplimiento de la ley para iniciar investigaciones. Si usted o sus hijos fueron engañados por una estafa phishing, reporte el incidente en **ReporteFraude.ftc.gov.**

PROTEJA LA PRIVACIDAD DE SUS HIJOS

Como padre, usted tiene el 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 Regla 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 Regla 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 Regla 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 estos 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, por ejemplo:

- nombre
- domicilio
- número de teléfono o domicilio de email
- paradero físico
- número de Seguro Social
- fotos, videos y grabaciones de audio del niño
- identificadores persistentes, como domicilios IP, que se pueden usar para hacer un seguimiento de las actividades de un niño con el transcurso del tiempo y en distintos sitios web y servicios en línea

¿Cómo funciona la Regla 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 podría hacer con la información — por ejemplo, si el sitio prevé usar la información para enviarle publicidad a un niño, o si les 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 con respecto al método a utilizar para obtener su consentimiento. Por ejemplo, pueden pedirle que remita una hoja de permiso.

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 la 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 se elimine 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 **ReporteFraude.ftc.gov**.

ftc.gov/ninosenlinea

Para ordenar folletos sobre cómo proteger a los niños cuando están en línea, visite **FTC.gov/ordenar**.

PARA | PIENSA | CONÉCTATE®

Comisión Federal de Comercio (FTC) // Febrero 2019