Learning.com
EXCEL IN A DIGITAL WORLD

Guía de Seguridad en-línea para Padres
Definiciones, Herramientas, Consejos y Recursos

La tecnología está cambiando más rápido de lo que muchos de nosotros podemos estar al tanto y requiere vigilancia para mantenernos al ritmo de definiciones, herramientas, riesgos, y recursos acerca del mundo en-línea. Esta guía para padres cubre varios de los temas de seguridad en línea para equipar a los padres con información y recursos necesarios para estar informados acerca de la Web. Específicamente, este recurso cubre información acerca de filtros, protección de virus, teléfonos celulares, privacidad en línea, depredadores, propiedad intelectual, etiqueta de la red, ergonomía y comportamiento adictivo. También incluye herramientas útiles para poner reglas y expectativas, tal como el contrato de seguridad en línea.

Después de leer este manual de los padres, platique con su familia y llegue a un acuerdo acerca de su propia "póliza aceptable" en su casa. El contrato de seguridad en línea ayuda a dirigir la discusión y confirma el compromiso de la familia a seguir las reglas de su casa. Finalmente, use los útiles consejos y recursos para ampliar su investigación acerca de seguridad en línea para que usted y su familia puedan disfrutar de todos los beneficios de la tecnología y estar seguros de que han hecho lo que está en sus manos para mantenerse seguros en este mundo de cambios.

Nota: Para aprender más acerca del acoso cibernético vea la Guía para Padres Easy Tech de Acoso Cibernético.

Filtros

Definición:

Los filtros limitan a donde puede ir la gente y lo que puede hacer en línea. Pueden bloquear el acceso a ciertos sitios, o a ciertos medios de comunicación como correo electrónico, chat o mensajes instantáneos. También pueden monitorear lo que hacen los menores en línea, y controlar la cantidad de tiempo que pasan ahí. Muchos buscadores en línea ofrecen opciones de filtros que bloquean cualquier resultado de búsquedas que los padres creen inapropiados.

Herramientas de Filtros:

- **Filtrar descripciones gráficas o imágenes explícitas:** Estas herramientas bloquean a las personas para evitar que vean material sexualmente explicito en la Web. Pero tenga cuidado, ningún filtro es perfecto.
- Monitorear actividades en línea: Estas herramientas permiten a los padres y cuidadores monitorear actividades en línea mediante una variedad de métodos.
- Limitar la cantidad de tiempo que se pasa en línea: Estas herramientas pueden limitar la cantidad de tiempo que se pasa en línea. Algunas herramientas permiten a los padres bloquear horas del día cuando una persona puede o no conectarse a la Internet.
- Bloquear información para prevenir que sea publicada o mandada por correo electrónico: Estas herramientas previenen que la gente de su información personal (como nombre, dirección de su casa, etc.) a personas extrañas mientras este en línea.
- Navegador para niños: Estos son navegadores de Internet que sirven como una puerta entre la computadora y la Internet. Los navegadores para niños generalmente filtran palabras o imágenes de contenido sexual o de otra manera inapropiadas. Con frecuencia son diseñados

para ser más fáciles de usar para los niños.

Consejos para usar Filtros:

- Tenga una plática entre familia e investigue acerca de los mejores tipos de filtros para su familia. Haga un acuerdo con su hijo(a), estableciendo una guía y reglas para el uso aceptable de la computadora.
- Califique las categorías de filtros y características basados en que tan importantes son para mantener a su familia segura mientras mantiene la cantidad de libertad en línea que su hijo(a) quiere.

Propiedad Intelectual

Definición:

La propiedad intelectual (IP) se refiere a las creaciones de la mente – inventos, trabajos literarios y artísticos, símbolos, nombres, imágenes y diseños usados en el comercio. Al compartir archivos o mediante programas de redes entre pares, los niños pueden se pueden encontrar con propiedad intelectual, frecuentemente en la forma de música, películas, videos o programas de TV con derechos de autor.

Riesgos:

- Los usuarios de programas para compartir archivos pueden estar en violación de la ley de derechos de autor cuando intercambian o hacen varias copias de musca, películas, videos o programas de TV con derechos de autor.
- Muchos programas para compartir archivos o de redes entre pares ofrecen acceso fácil, y hasta accidental a videos e imágenes ilegales.
- Los sitios para compartir archivos y sitios de redes entre pares ponen su computadora en riesgo de dar a otros, acceso a su computadora.
- Cuando usted baja programas para compartir archivos a su computadora, usted también puede estar bajando software adicional conocido como “spyware”. Los anunciantes y pornógrafos usan spyware para generar tráfico en sus sitios Web.

Consejos para los padres:

- Hable con su hijo acerca de la propiedad intelectual y las leyes de copyright o derechos de autor. Asegúrese de que ellos sepan qué es legal y qué es ilegal.
- Investigue las opciones legales y gratis o legales con pago para descargar archivos. Dígale a su hijo(a) las opciones que existen para descargar archivos legalmente. Marque estos sitios para tener acceso fácil a ellos.
- Trate de usar MP3s libres de derechos para mantenerse alejado de virus de computadoras y cumpla con las leyes de copyright. La mayoría de programas para compartir archivos le permite escoger el tipo de archivos que quiere buscar. Usualmente, su hijo debería buscar archivos de música (MP3s) y no videos archivos de imágenes.

- Asegúrese de que tenga instalado software de anti-virus y firewalls actualizados para protección de virus.

Etiqueta de la Red

Definición:

Etiqueta de la red se refiere a las guías de comportamiento y comunicación aceptables en línea. La etiqueta de la red establece guías que ayudan a la gente a comunicarse efectiva y responsablemente y de una manera segura.

Lo que su hijo(a) debe saber:

- La responsabilidad de usar la Internet y la póliza de uso aceptable de la escuela.
- Cuando la gente se comunica sin verse cara a cara o sin escuchar sus voces, puede ser difícil saber si las personas están enojadas o contentas.
- La gente usa diferentes métodos para comunicar sus emociones mediante la tecnología:
    - Caras con símbolos para mostrar cómo se sienten. Tal como :) para mostrar que están sonriendo o contentos, y :(cuando están tristes.
    - Escribir con letras mayúsculas puede comunicar que la persona esta gritando.
- Los mensajes con intención de hacer a su hijo(a) sentir mal no son aceptables. Su hijo(a) no debe responder y debe enseñar el mensaje a un adulto de confianza, tal como un maestro.
- Su hijo nunca debe tratar de hacer daño a nadie escribiendo algo malo, y su hijo debe decirle a usted o a un maestro cuando alguien está tratando de hacerle daño a alguien más. Su hijo(a) nunca debe escribir algo que él o ella no dirían a alguien en persona.
- La comunicación en línea nunca debe ser usada para hacerle daño a otra persona al difundir rumores o decir cosas malas.
- Su hijo(a) sólo debe enviar o publicar algo que usted aprobaría. Cualquier cosa enviada usando la tecnología puede hacerse visible a todos en el mundo, y hasta podría ser usada por alguien para hacerle daño a su hijo(a) cualquier día, ahora o en el futuro.

Consejos para los padres:

- Haga una póliza aceptable para los miembros de su casa que concuerda con la póliza de la escuela.
- Platique acerca de artículos en las noticias sobre los usos buenos y malos de la Internet.
- Practique escribiendo mensajes de correo electrónico con su hijo(a) para reforzar y modelar las reglas apropiadas de la etiqueta de la red.

Ergonomía

Definición:

La ergonomía es el estudio del trabajo. Trata de desarrollar equipo o herramientas para facilitar el trabajo. Para niños que están en la computadora, enviando mensajes de texto, o jugando video juegos con frecuencia, la ergonomía puede ser importante para su salud y seguridad.

Riesgos:

- La ergonomía inapropiada en computación puede causar el síndrome del túnel carpiano.
- El enviar demasiados mensajes de texto puede causar tendinitis de adolescentes, la cual es el principio del síndrome del túnel carpiano.
- Lesiones al dedo pulgar también pueden resultar del uso continuo de asistentes personales de mano (PDAs) con teclados pequeños y por el movimiento repetitivo al jugar video juegos.
- La silla incorrecta y/o la altura del escritorio mientras se usa la computadora pueden causar dolor de espalda y cuello.

Consejos para los padres:

- Haga que su hijo use una plataforma para el teclado y el mouse. Estas están diseñadas para tener mejor postura y deben ser colocadas a un ángulo que mantiene las muñecas en una posición horizontal.
- Asegúrese de que la silla y escritorio que su hijo(a) usa para la computadora son de la altura correcta, soportan la espalda y no causan tensión en el cuello.
- Dígale a su hijo(a) que el enviar muchos mensajes de texto puede causar tendinitis de adolescentes, la cual es el principio del síndrome del túnel carpiano.
- Explíquele los síntomas del síndrome del túnel carpiano a si hijo(a), para que esté consciente de los síntomas.
- Coloque consejos de seguridad ergonómica cerca de la computadora para recordarle a su hijo(a) la postura correcta.

Comportamiento Adictivo

Definición:

El comportamiento adictivo ha sido usado para definir el uso excesivo de la Internet. El comportamiento adictivo es asociado con el no poder dejar de entrar en línea a tal punto que causa un impacto en otras áreas de su vida, incluyendo amistades, relaciones con la familia, estabilidad emocional, la escuela etc.

Señales de advertencia:

- El trabajo de la escuela del niño(a) está siendo afectado.
- Las amistades y las relaciones cercanas son descuidadas o afectadas de una manera negativa.
- El juego o actividad en línea está tomando la mayor parte del tiempo libre del niño(a) y lo prefiere en lugar de otras actividades o eventos.
- El niño(a) se enoja o muestra comportamiento errático cuando no puede jugar el juego o entrar en línea.
- Cuando se le pregunta acerca de la cantidad de tiempo que pasa, esconde su actividad.
- Descuida su espacio o aseo personal.

Consejos para los padres:

- Considere todos los factores antes de calificar a su hijo de tener comportamiento adictivo.
- Mantenga un diálogo abierto. Hable con su hijo(a) frecuentemente acerca de todas las actividades en su vida e inclúyalo en eventos regulares para mantener la consistencia y garantizar algo de tiempo retirado de la tecnología.
- Promueva el uso saludable del teléfono. Haga que su hijo(a) se tome el tiempo para desconectarse de su teléfono o computadora. Trabaje con él o ella para establecer límites de cuánto tiempo él o ella pasa enviando mensajes de texto en el teléfono y/o computadora. Escoja un tiempo cada día, para "desconectarse" y participar en otras actividades.
- Investigue acerca del software que monitorea el uso de la Internet. Estas herramientas pueden ser útiles en recordarle a su hijo(a) cuanto tiempo ha estado en la computadora para que pueda aprender a monitorear y ajustar su propio comportamiento y empezar a tener hábitos mas saludables. (Vea la Sección de Filtros para más información.)
- Mantenga las computadoras con acceso a Internet en un espacio compartido. Cuando los niños(as) usan una computadora en un cuarto compartido con otros miembros de la familia, es más probable que regulen su uso y comportamiento ellos mismos.
- Monitoree su propio uso de la computadora y teléfono celular. Su comportamiento es un modelo para su hijo(a) y puede servir como una buena guía para el uso responsable de la tecnología.
- Busque ayuda si ve un comportamiento adictivo. Si su hijo(a) muestra comportamiento adictivo, considere llevarlo(a) a un consejero. La adicción a la Internet puede ser síntoma de otros problemas como depresión o enojo. Si su hijo(a) habla con un profesional, le puede ayudar a revelar los problemas más profundos que pueden estar creando este comportamiento.

Protección de Virus

Definición:

La protección de virus ayuda a una computadora en contra de aplicaciones intrusivas. Estas aplicaciones intrusivas incluyen virus, worms o gusanos, spyware y anuncios de ventanas emergentes. Si no está protegida, una computadora se hace vulnerable a ataques por parte de aplicaciones intrusivas y la información puede ser destruida y perdida y la información personal y contraseñas robadas. Estas aplicaciones intrusivas pueden afectar la salud de toda su computadora.

Tipos y ejemplos de aplicaciones intrusivas:

- Virus – Un virus es una pieza de software que se basa en un programa real. Por ejemplo: Un virus se adjunta a un programa en su computadora, tal como un programa de hoja de datos. Cada vez que corre el programa de hoja de datos el virus corre también y tiene la oportunidad de reproducirse (al adjuntarse a otros programas).
- Worm – Un worm (o gusano) es una pequeña pieza de software que usa las redes de computación o fallas de seguridad para copiarse a sí mismo. Una copia del worm busca en la red otra máquina que tenga un fallo de seguridad específico. Se copia a sí mismo a la nueva máquina usando la falla de seguridad y de ahí se empieza a replicar también.Por ejemplo, usted está usando una de las computadoras de la escuela y una pantalla de seguridad se

abre diciéndole que necesita correr una actualización. La pantalla se ve legítima, pero cuando se fija de cerca, no concuerda exactamente con el tema de la computadora. Pensando que es legítima, usted hace clic e infecta la computadora con un worm. El worm encuentra otra computadora en la red y corre la misma pantalla de seguridad falsa.

- Anuncios de ventanas emergentes – Son aplicaciones que abren una nueva ventana del navegador de Internet con un nuevo contenido. La ventana nueva aparece sobre su pantalla actual, cubriendo la página Web que usted quiere ver. Hacer clic en el anuncio puede crear más anuncios o peor, traer aplicaciones intrusivas como spyware o virus.
- Por ejemplo: Usted está buscando direcciones en la Web y aparece un anuncio de repente. Su computadora se infecta con un virus. El virus sigue generando nuevos anuncios sin parar y hace que su navegador de Web esté tan lento que ya no se puede usar.

Spyware – Estos programas de computación de verdad lo "espían". Las aplicaciones de spyware se quedan silenciosamente en su computadora e interceptan información personal tal como nombres de usuario y contraseñas.

Por ejemplo: Usted está buscando animales en su sitio Web favorito y un anuncio de una película aparece en su computadora. Parece interesante, así es que usted le hace clic e infecta su computadora con spyware.

Riesgos:

- Instale una forma de protección contra virus de confianza para defenderse de aplicaciones intrusivas. Sin software de protección de virus, usted se expone, y expone a su computadora a ataques, robo de identidad y malware de computadoras.

Consejos para los padres:

- Use los Recursos de protección de virus (al final de este documento) para ayudarle a investigar acerca del mejor software de protección de virus para su computadora.
- Como familia, investigue y revise aplicaciones y escoja una para proteger su computadora.
- Haga una junta de familia para platicar sobre los ejemplos de aplicaciones intrusivas, como se ven y lo que NO hay que hacer cuando este tipo de aplicaciones aparecen, o lo que hay que hacer cuando un programa de protección de virus detecta una aplicación intrusiva.

Seguridad del Teléfono Celular

Definición:

La seguridad del teléfono celular se enfoca en cómo prevenir y proteger a una persona de situaciones potencialmente dañinas cuando se trata de teléfonos celulares y el envió de mensajes de texto a través un celular. Los niños deben saber cuál es el uso apropiado y seguro de un teléfono celular.

Información general y Riesgos acerca de los Mensajes de Texto:

- Dígale a su hijo(a) que no publique números de teléfono en línea, o se puede hacer vulnerable al acoso cibernéntico, a criminales que quieren conocerlo en persona y a estafas o scams.

- Platique con su hijo y dígale que él o ella nunca puede estar 100 por ciento seguro de que la persona que está enviando el mensaje de texto sea la dueña del teléfono.
    - Dígale a su hijo(a) que no envié información personal a través de un mensaje de texto (acerca de él, ella u otros); el teléfono al que él o ella estén enviando el mensaje de texto puede haber sido robado.
    - Dígale a su hijo que nunca envié una contraseña o numero de identificación personal a un amigo; la persona que le esté pidiendo esta información puede haber robado el teléfono.
    - Explíquele a su hijo que si alguien le envía un mensaje de texto para verse, aunque la persona sea un amigo conocido, le debe llamar para confirmar; el teléfono puede haber sido robado.
- Dígale a su hijo que nunca deje que alguien desconocido use su teléfono celular porque esa persona puede hacer bromas llamando por teléfono o enviando un mensaje de texto.
- Explíquele a su hijo que si alguien que él o ella conoce necesita usar el teléfono para una emergencia o razón importante (tal como llamar a un padre) su hijo debe tener cuidado y ver lo que hace la otra persona, para asegurarse de que él o ella no se hace pasar por su hijo.
- Dígale a su hijo que ignore enlaces que no esperaba, archivos, fotos y teléfonos y que solo los abra cuando son enviados por una persona conocida y su hijo(a) sabe por qué fueron enviados.
- Explíquele a su hijo que solamente envié textos o responda a la gente que él o ella conoce. Si el número es desconocido, ignore el mensaje de texto y trate de encontrar quién lo mando. Dígale a su hijo que piense antes de enviar un mensaje de texto, y que nunca mande un texto diciendo lo que él o ella no diría en persona.
- Dígale a su hijo que siempre piense en cómo se sentiría alguien antes de enviarle un texto.
- Si su hijo está enojado, dígale que espere antes de enviar un texto para evitar que mande mensajes ofensivos o dañinos.
- Dígale a su hijo que si alguien le manda un mensaje ofensivo o dañino, no lo conteste y se lo enseñe a un maestro antes de borrarlo.ar
- Dígale a su hijo que nunca trate de lastimar a alguien o ayudar a alguien a lastimar a alguien más enviándole mensajes de texto o fotos.
- Explíquele a su hijo(a) que cualquier cosa que es enviada electrónicamente puede ser re-enviada, publicada en línea, y usada para lastimar a su hijo(a), ahora o en el futuro. La información en línea puede hacerse pública para que todo el mundo la vea, permanentemente.
- Dígale a su hijo(a) que nunca envié un texto que le pueda hacer daño o causar vergüenza.

Seguridad General para el uso del Teléfono

- Explíquele a su hijo que no envié textos mientras camina.
- Nunca envíe un mensaje de texto o hable por el celular mientras maneja.
- Dígale a su hijo(a) que el envío excesivo de mensajes de texto puede causar tendinitis de adolescentes, la cual es el principio del síndrome del túnel carpiano.

- Explíquele los síntomas del síndrome del túnel carpiano y que él o ella debe decirle si tiene esos síntomas.

Consejos para los padres:

- Use un contrato como el Contrato de mensajes de texto, al final de este documento, para establecer las expectativas y reglas que su hijo(a) debe seguir. Establezca consecuencias razonables que deben ser llevadas a cabo si las expectativas del contrato no son cumplidas.
- Involucre a su hijo en el proceso de selección de un plan y teléfono celular para que él o ella entienda los costos asociados con tener un teléfono celular así como las características y limitaciones del plan que fue escogido.
- Revisen las facturas mensuales juntos para ponerle un alto a las llamadas excesivas y costos adicionales por acceso a Internet o por la compra de aplicaciones (apps) o tonos de timbre (ringtones).
- Mantenga un diálogo abierto con su hijo(a) acerca de situaciones potencialmente dañinas para que él o ella tenga un lugar a donde recurrir si él o ella siente que puede estar en problemas, o está preocupado(a) acerca de una situación. Asegúrese de que él o ella sepan que usted está ahí para él o ella sin importar la falta o situación.
- Si usted no es un experto en enviar mensajes de texto, pídale a sus hijos que lo enseñen. Usted podrá encontrarlo como un método de comunicación fácil y eficiente.
- Vigile y observe el uso del teléfono celular. Asegúrese de hablar con su hijo(a) acerca de patrones negativos que usted vea antes de que se empeoren o se conviertan en dañinos.

Privacidad en línea

Definición:

La privacidad en línea se refiere a la manera en que nos protegemos como individuos del robo de identidad así como también a como mantenemos nuestra información personal segura. El robo de identidad es cuando una persona toma información personal de otra y la hace suya. El robo de identidad y el fraude de identidad son términos usados para referirse a todo tipo de crímenes en donde alguien maliciosamente obtiene y usa la información personal de otra persona de una manera que se convierte en fraude o engaño, generalmente para obtener ganancias monetarias.

Ejemplos de Robo de Identidad en Línea:

- Robo de Identidad de Tarjeta de Crédito – Los criminales que obtienen acceso a números de tarjetas de crédito pueden hacer compras y arruinar el crédito de las personas por años. Platique con su hijo(a) sobre como el proteger la identidad de los miembros de su familia es una responsabilidad compartida de todos los miembros de la familia.
- Robo de Número de Seguro – Los criminales de la red que acceden los números de seguro social pueden usar los números para crear una nueva identidad o solicitar crédito. Esto podría dañar el crédito por años. Dígale a su hijo(a) que no de su seguro social en línea.
- Robo de Personalidad – Platique con su hijo(a) acerca de las formas y consecuencias del robo de personalidad. Explíquele que alguien podría usar una dirección de correo electrónico para hacerse pasar por alguien y dañar a otros. Este tipo de robo puede ser dañino a la

integridad y reputación de una persona. Comúnmente, a los niños con contraseñas débiles les han robado sus avatares en sitios de juego en línea.

Prevención del Robo de Identidad:

- Explíquele a su hijo que él o ella nunca debe usar información tal como fecha de nacimiento, número de seguro social, o el nombre de soltera de su mamá como contraseña o nombre de usuario para ninguna de sus cuentas en línea.
- Eduque a su hijo(a) para no dar información personal en salas de chat o en sitios redes sociales que permiten a los miembros publicar abiertamente su dirección y teléfono ante todos los que visiten su perfil.
- Platique sobre las reglas de uso del teléfono celular que previenen el robo de identidad (vea la Sección de Seguridad de Teléfono para más información). Recuérdele a su hijo(a) que no preste su teléfono a otros y que nunca envíe un correo electrónico o texto al gente desconocida.
- Explíquele que algunos sitios son seguros, pero otros no. Su hijo(a) siempre debería revisar si la seguridad de un sitio es auténtica antes de ingresar cualquier información personal.
    - Use un buscador como Google para llegar al sitio y asegurarse de que usted escribió la dirección Web correctamente.
    - Siempre busque “https:” en cualquier sitio que le permite ingresar información delicada.
    - Vea el URL en el navegador, ¿es el sitio correcto?
    - Nunca envíe su nombre de usuario y contraseña o cualquier otra información delicada en un mensaje de correo electrónico.

Consejos para los padres:

- Las investigaciones en el campo de seguridad muestran que los tres comportamientos que lo ponen en más riesgo en línea son:
    - Hablar de sexo
    - Ponerse de acuerdo en verse con alguien que conoció en línea
    - Molestar a otros en línea
- De manera alarmante, en la mayoría de los casos de depredadores, el depredador concia al niño en la vida real.
- Usted es la primera línea de defensa para proteger la privacidad en línea de su hijo(a).
- Platique con su hijo(a) sobre la importancia de la información personal.
- Asegúrese de que su hijo(a) deje solamente la mínima información personal en cualquier sitio Web.
- Marque los sitios no comerciales de alta calidad para su hijo que sean divertidos y educativos, y úselos como opciones para cuando su hijo esté en la computadora.
- Mientras visite y use sitios de redes sociales, asegúrese de que sus ajustes de privacidad estén puestos para que sólo sus amigos puedan ver el perfil de su hijo(a). Revise los ajustes de su hijo(a), ya que pueden ser confusos o engañosos. Revise los ajustes de su hijo(a) periódicamente ya que estos sitios pueden cambiar los ajustes de privacidad con el tiempo.

- Compre en línea con su hijo(a). Asegúrese de que cualquier sitio que usted use tenga requisitos para asegurase de que las transacciones son seguras. Muéstrele a su hijo como sitios con codificación muestran http en la barra de dirección en lugar de http.
- Regístrese con su hijo en diferentes sitios Web.

Depredadores

Definición:

Los depredadores en línea encuentran a los niños mediante redes de sitios sociales, blogs, salas de chat, mensajes instantáneos, correo electrónico, paneles de discusión, sitios de juego y otros sitos Web. Ellos seducen a sus blancos con atención, amistad y gentileza y a veces hasta con regalos. Ellos conocen la música de moda y los hobbies que les interesan a los niños. Se prestan para "escuchar" y están al tanto de los problemas de los niños. Estos depredadores gradualmente introducen contenido sexual en sus conversaciones y pueden eventualmente mostrar material sexualmente explícito. La amenaza más grande es que estos depredadores tratan de encontrar la manera de verse con el niño cara a cara tarde o temprano.

De acuerdo al Centro de reporte de seguridad en Internet Berkman, basado sobre la investigación hecha por Wolak, Finkelhor, y Mitchell and M. Ybarra, los niños que están en más riesgo son de las edades entre 12 y 17. Son generalmente niñas, gay, o tienen dudas sobre su identidad sexual. Los niños que han sido abusados sexualmente en el pasado también tienen un riesgo mayor.

Los jóvenes que son el blanco inapropiado de adultos están generalmente buscando material sexual o hablando de sexo en línea. Han visitado salas de chat para adultos, donde las conversaciones se tornan sexuales. Ayudar a los jóvenes a evitar estos sitios y ayudarles a presentarse de una forma no sexual rápidamente en línea es importante.

Consejos para los padres:

- Hable con su hijo(a) acerca de los depredadores en línea y acerca de lo que se proponen hacer. Explíqueles que la mayoría de la gente que conocemos en línea es amigable, pero que algunos individuos pueden ser malos o pueden querer lastimar a otros.
- Hable con su hijo acerca de las relaciones saludables.
- Esté alerta a los señales que se presenten si su hijo(a) se está involucrando en comunicación inapropiada con adultos en línea. Algunas señales que pueden ocurrir si su hijo es el blanco son:
    - El o ella se pasa mucho tiempo en línea solo(a).
    - Usted encuentra pornografía o fotografías sexuales en la computadora de la familia.
    - El o ella recibe llamadas de gente que usted no conoce, o hace llamadas (algunas veces de larga distancia) a números que no reconoce.
    - El o ella recibe correo, regalos o paquetes de alguien que usted no conoce.
    - El o ella se aleja de familia y amigos, o rápidamente apaga el monitor o cambia la pantalla cuando algún adulto entra al cuarto.

(Adaptado del sitio Web www.bewebaware.ca/english/sexual_risks_harm.html.)

Learning.com
EXCEL IN A DIGITAL WORLD

- Hable con su hijo acerca de quien en su círculo es considerado un adulto responsable y de confianza. Platique con otros adultos en los que él o ella puede confiar, tales como maestros, directores, entrenadores, etc.
- Use software de control parental.
- Mantenga la computadora en una área común de la casa para que pueda ser vista por otros. Siéntese frecuentemente con su hijo(a) mientras él o ella está usando la Internet.
- Platique sobre la importancia de comunicación abierta y sobre qué puede pasar cuando su hijo(a) guarda un secreto o no comparte la información. Explíquele que nadie le puede decir que guarde secretos con usted, y que si le dicen que lo haga, su hijo(a) debe decírselo a usted ¡inmediatamente!
- Dele a su hijo(a) consejos e ideas para comunicarse sobre de temas que pueden ser difíciles. Use los recursos como www.kidshealth.org para obtener consejos acerca de los niños y de cómo empezar una conversación difícil con los padres u otro adulto.
- Asegúrese de que su hijo mantenga su número privado. Ya que tantos clientes de mensajes instantáneos ahora hacen posible enviar mensajes directamente a los teléfonos celulares, nunca publique un teléfono celular en un sitio de red social o en ningún otro sitio.
- Asegúrese de que su hijo(a) limite los lugares donde su información personal sea publicada. Tenga cuidado de quien puede acceder su información para reducir el exponerse a gente que él o ella no conoce. Esto protegerá su privacidad y reducirá el contacto de gente extraña, busca pleitos, o depredadores potenciales.

Learning.com
EXCEL IN A DIGITAL WORLD

Contrato de Seguridad en Línea de Nuestra Familia

Después de leer la guía para padres, platique con su familia para llegar a un acuerdo acerca de su propia "póliza aceptable" dentro de su casa. Este contrato le ayudará a guiar su discusión y a confirmar el compromiso para seguir las reglas de estar en línea en su casa.

Nombre de partes interesadas

Este contrato es entre _____ y _____

Declaración del acuerdo_____

_____

Términos del acuerdo

Ergonomía: ¿Cómo modificaremos nuestro entorno para trabajar con seguridad con aparatos electrónicos?_____

_____

_____

_____

Filtros: ¿Cuáles filtros son necesarios en nuestra familia para hacer uso de la computadora de una manera segura y responsable? _____

_____

_____

_____

Protección de Virus: ¿Qué tipo de protección de virus usará nuestra familia para proteger nuestra computadora de aplicaciones intrusivas? _____

_____

_____

_____

Teléfonos Celulares: ¿Qué reglas deberemos seguir al enviar mensajes de texto y al hablar por teléfonos celulares? _____

_____

_____

_____

Learning.com
EXCEL IN A DIGITAL WORLD

Privacidad en-línea: ¿Cuáles pasos seguiremos para proteger a nuestra familia del robo de identidad y para mantener nuestra información personal protegida?

_____

_____

_____

_____

Depredadores: ¿Cómo podemos mantener una comunicación abierta y ser proactivos acerca de situaciones peligrosas y/o encuentros con depredadores?

_____

_____

_____

_____

Propiedad Intelectual: ¿Qué reglas y guías vamos a seguir para no violar la ley cuando usamos programas para compartir archives o programas de redes entre pares?

_____

_____

_____

_____

Netiquette: What kind of acceptable online behavior will our family use to be safe, respectful, and Etiqueta de la Red: ¿Qué tipo de comportamiento aceptable usará su familia para estar seguro y ser respetuoso y responsable en línea?

_____

_____

_____

_____

Comportamiento Adictivo: ¿Qué reglas seguiremos para promover el uso saludable dela tecnología? ¿Cómo nos aseguraremos que vamos a seguir estas reglas?

_____

_____

_____

_____

Al firmar esto estamos de acuerdo a acatar y seguir los terminus mencionados.

Firma:_____y _____

Fecha _____

Learning.com
EXCEL IN A DIGITAL WORLD

Contrato de Mensajes de Texto

Nombre de partes interesadas

Este contrato es entre _____ y _____

Declaración del acuerdo_____

_____

Términos del acuerdo

Ergonomía: ¿Cómo cambiarás en cuanto a enviar mensajes de texto para mantenerte seguro?

_____

_____

_____

_____

Prevención: ¿Cómo evitarás situaciones potencialmente dañinas?

_____

_____

_____

_____

Acciones de Seguridad: Explica cuales acciones tomarás para protegerte.

_____

_____

_____

_____

Comportamiento Social: Enumera las reglas que seguirás al mandar mensajes de texto.

_____

_____

_____

_____

Al firmar esto estamos de acuerdo a acatar y seguir los terminus mencionados.

Firma:_____ y _____

Fecha _____

Learning.com
EXCEL IN A DIGITAL WORLD

Recursos

Filtros

GetNetWise
http://kids.getnetwise.org/tools/tool_result.php3

Padre
Esta página Web ofrece un portal para buscar diferents tipos de herramientas y recursos de Internet, incluyendo navegadores para niños, filtros, redes entre pares y muchos otros.

Common Sense Media
http://www.commonsensemedia.org/tech-tip-using-google-safe-search

Padre
Esta página Web proporciona un video de cómo establecer la opción de búsquedas seguras en Google.

Propiedad Intelectual

Media Awareness Network
http://www.media-awareness.ca/english/parents/index.cfm

Padre
Esta página Web incluye recursos y apoyo para padres y maestros interesados en publicaciones e información impresa para niños. Incluye investigaciones, planes de lección, blogs y productos para apoyar el hacer conciencia acerca de los medios de comunicación.

World Intellectual Property Organization
http://www.wipo.int/about-ip/en/

Padre
Esta página Web le da una explicación clara y detallada para responder a la pregunta ¿"Qué es Propiedad Intelectual?" Usted encontrará enlaces para descargar el manual de Propiedad Intelectual así como también un documento llamado Entendiendo los derechos de copyright y otros relacionados.

U.S. Copyright Office
http://www.copyright.gov/

Padre
Este es el sitio Web de copyright de los Estados Unidos, y muestra toda la información acerca de licencias de copyright, leyes y pólizas, incluyendo una sección acerca de temas básicos de copyright y preguntas frecuentes.

Etiqueta en la Red

CyberSmart!
http://cybersmartcurriculum.org/mannersbullyingethics/

Padre
El sitio Web CyberSmart's se enfoca en las aptitudes del siglo 21 para educación. Esta página Web se concentra en la conducta y comportamiento cibernético. Hay varios recursos que explorar, incluyendo planes de lección y tareas para llevarse a casa.

Ergonomía

Safe Computing Tips
http://www.safecomputingtips.com/articles/ergonomic-technology.html

Padre
Este artículo de SafeComputingTips.com se enfoca en tener un ambiente saludable y evitar lesiones mientras trabaja largas horas en la computadora.

Carpal Tunnel Syndrome – Symptoms – MayoClinic.com
http://www.mayoclinic.com/health/carpal-tunnel%20syndrome/DS00326/DSECTION=symptoms

Padre, 6–8, 9-12
Esta página Web muestra la definición y los síntomas del síndrome del túnel carpiano. También proporciona enlaces a otras investigaciones con enlaces a: causa, factores de riesgo, diagnósticos, tratamientos, remedios caseros medicina alternativa, como lidiar, apoyo y prevención.

Compartir Archivos

FBI
http://www.fbi.gov/cyberinvest/cyberedletter.htm

Padre, 6–8, 9-12
Esta carta del FBI muestra los riesgos y peligros de usar sistemas de red por pares. Explica los tres crímenes más comunes asociados con los sistemas de red por pares – copyright, violación de copyright, explotación de menores y piratería informática.

Media Awareness Network
http://www.media-awareness.ca/english/resources/special_initiatives/wa_resources/wa_teachers/are_you_web_aware/web_aware_filesharing.cfm

Padre, 3–5, 6–8, 9-12
Este sitio Web se titula "¿Estás al tanto de la Web? Compartir archivos," está escrito en un lenguaje para niños. Explica los usos positivos y negativos de compartir archivos. Da estadísticas, definiciones

y estrategias para hacer el compartir archivos una experiencia positiva. Esta es una organización canadiense, así es que algunas estadísticas y leyes son presentadas desde la perspectiva canadiense.

SoftForYou
http://www.softforyou.com/articles_tutorials/peer_to_peer_networks.html

Padre
Este sitio Web tiene un artículo llamado “Redes de pares: Información vital para los padres” por Jonathan Stromberg. Este artículo explica qué son las redes de pares, por qué son populares, los peligros asociados con ellas, y los sitios más comunes de redes de pares.

TopTenREVIEWS
http://internet-filter-review.toptenreviews.com/peer-to-peer-file-sharing.html

Padre
Este sitio Web explica las redes de pares y como se usan. Explica por qué estos sistemas deben ser de cuidado. También enumera los sitios Web más comunes para compartir archivos. Se muestran capturas de pantallas de contenido controvertido siendo compartido.

Wikipedia
http://en.wikipedia.org/wiki/File_hosting_service

Padre, 6–8, 9-12
Esta es la entrada para “servicios de alojamiento de sitios Web.” Se enfoca en explicar el lado técnico de los servicios de alojamiento de sitios Web. Presenta una gráfica que compara los servicios de alojamiento más comunes.

Mensajes de Texto

Connect Safely
http://www.connectsafely.org/

Padre, 3–5, 6–8, 9-12
Este sitio Web proporciona numerosos consejos de seguridad en cuanto a tecnología. Asuntos relacionados con mensajes de texto como sexting y seguridad en el celular están bien explicados, pero otros consejos de seguridad relacionados a asuntos, como compartir videos y salas de chat, también están disponibles.

Education.com
http://www.education.com/magazine/article/child-sexting-parents

Padre, 6–8, 9-12
This article includes information for parents about sexting. It explains what it is, consequences for sexting, and tips for parents about how to keep their children safe from sexting.

Examiner.com

http://www.examiner.com/x-931-NY-Parenting-Teens-Examiner~y2009m1d17-Teen-Texting-Safety-Tips

Padre, 3–5, 6–8, 9-12
Este sitio Web incluye cinco consejos de seguridad sobre mensajes de texto entre adolescentes. Estos consejos pueden ayudar a los niños a entender como estar seguros con sus teléfonos celulares. También tiene un enlace a mas información acerca del "lenguaje" de mensajes de texto.

KidsHealth

http://www.kidshealth.org/teen/safety/safebasics/texting.html

Padre, 3–5, 6–8, 9-12
Este artículo explica los peligros de enviar textos mientras "estas en movimiento," como caminando o manejando. El sitio Web da ejemplos de lo peligroso que es enviar o recibir textos mientras estas en movimiento, tales como accidentes de carros. Incluye consejos sobre cuando enviar mensajes y cuando no.

KidsHealth

http://kidshealth.org/teen/safety/driving/no_texting.html

Padre, K–2, 3–5, 6–8, 9-12
Este sitio Web da a los niños el lenguaje que pueden usar para animar a otros a no enviar textos mientras manejan. Este artículo se relaciona a los estudiantes demasiado jóvenes para manejar, porque les dice lo que pueden hacer como pasajeros de un carro para ayudar a la gente a dejar de enviar textos al manejar aunque ellos mismos sean muy jóvenes para manejar.

NetLingo

http://www.netlingo.com/acronyms.php

Padre
Este sitio Web ofrece una amplia lista de definiciones de acrónimos de Internet y el idioma que se usa en mensajes de texto.

Scholastic.com

http://content.scholastic.com/browse/article.jsp?id=3751903

Padre, K–2, 3–5
Este sitio llamado "Seguridad en el teléfono celular: Consejos útiles para comunicación entre niños," es para niños. El idioma es apropiado para ellos e incluye definiciones de palabras comunes relacionadas a teléfonos celulares, tal como "acosador cibernético" y "spammers o estafadores". Incluye los riesgos del uso del teléfono celular y maneras de usar el teléfono celular de una manera segura.

Learning.com
EXCEL IN A DIGITAL WORLD

Protección de Identidad

The Huffington Post
http://www.huffingtonpost.com/2010/01/21/worst-internet-passwords_n_431055.html

Padre, 3–5, 6–8, 9-12
Este artículo contiene información acerca de la creación de contraseñas fuertes. Enumera los 20 más comunes y por consiguiente peores contraseñas. Es un buen sitio Web para discutir cómo crear contraseñas buenas y fuertes con los estudiantes.

KidsHealth
http://kidshealth.org/kid/watch/house/online_id.html

Padre, 3–5, 6–8, 9-12
Este artículo de la Web trata el tema de "identidad en línea." Ayuda a los niños a considerar quienes son en línea y qué publicar en sitios de redes sociales. Utiliza lenguaje apropiado para niños y presenta reglas a seguir cuando se habla de la identidad en línea de las personas.

KidsHealth
http://kidshealth.org/teen/safety/safebasics/online_id.html

Padre, 3–5, 6–8, 9-12
Este artículo de la Web es acerca de la protección de su identidad en línea y de su reputación. Da ejemplos de las formas en que una identidad en línea puede afectar la vida de un niño, tal como ser expulsado de un equipo de deporte por publicar información inapropiada en un sitio de red social. Da a los niños cosas a considerar para mantener segura su identidad en línea y su reputación.

U.S. Department of Justice
http://www.justice.gov/criminal/fraud/websites/idtheft.html#whatis

Padre, 6–8, 9-12
This is a Web site created by the U.S. Department of Justice to explain identity theft. It includes the most common ways identity theft is committed and how to protect against identity theft.

Seguridad en Línea

American Association of School Librarians
http://www.ala.org/ala/mgrps/divs/aasl/aboutaasl/aaslcommunity/quicklinks/el/elinternet.cfm

Padre
Este sitio Web proporciona una lista de recursos que los maestros y los padres pueden usar para ayudar a los estudiantes a mantenerse seguros en línea. También incluye una discusión sobre los pros y contras de usar software de control parental para filtrar los sitos Web.

KidsHealth
http://kidshealth.org/teen/safety/safebasics/internet_safety.html

Padre, 3–5, 6–8, 9-12
Este artículo de la Web da información a los niños acerca de usar la Internet de una manera segura. Dice a los niños cómo mantener su información privada, cómo evitar ser acosados cibernéticamente, y cómo evitar enfados en línea.

KidsHealth
http://kidshealth.org/teen/your_mind/Parents/talk_to_parents.html

Padre, 3–5, 6–8, 9-12
Este artículo de la Web ayuda a los niños a entender cómo hablar con adultos. Incluye información acerca de cómo abordar un tema difícil con un adulto, el lenguaje que hay que usar para que los padres escuchen, y qué hay que hacer si el hablar con los padres no ayuda.

KidSites
http://www.kidsites.com/

Padre, K–2, 3–5
Este sitio Web conecta a los niños a sitios Web apropiados para ellos. El directorio incluye diferentes categorías donde los niños pueden encontrar información acerca de ese tema. Hay sitios educativos y sitios divertidos, y todos los sitos Web son apropiados para niños.

Media Awareness Network
http://www.media-awareness.ca/english/parents/index.cfm

Padre
Este sitio Web ofrece consejos para ayudar a los adultos a mantener a los niños seguros por edad, así que este es un lugar donde los maestros pueden encontrar información apropiada para diferentes edades para sus estudiantes. También hay información acerca de búsquedas en línea y enlaces a buscadores y directorios apropiados para niños.

U.S. Department of Homeland Security, US-CERT Cyber Security
http://www.us-cert.gov/cas/tips/ST05-002.html

Padre
Esta página Web presenta una lista de lo que los adultos pueden hacer para estar seguros en línea. La página también incluye enlaces a otros recursos relevantes a la seguridad en línea.

Comportamiento Adictivo

Be Web Aware
http://www.bewebaware.ca/english/default.html

Padre
Este sitio ofrece información y estadísticas acerca del uso excesivo de la Internet, incluyendo comportamiento adictivo asociado con los juegos en línea y los juegos de azar en línea.

Norton from Symantec
http://www.symantec.com/norton/library/familyresource/article.jsp?aid=fr_onlinegaming_addiction

Padre
Este artículo, titulado Jugadores en línea, Juegos vs. Adicción, ofrece descripciones de lo que es la adicción al juego y maneras de prevenirla.

Healthy Place
http://www.healthyplace.com/addictions/center-for-internet-addiction-recovery/addicted-to-online-gaming/menu-id-1111/

Padre
Esta página Web ofrece un artículo, una prueba, y ayuda en línea para tratar la adicción a juegos de computadora o de Internet.