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 etiqueta de la red, teléfonos celulares, filtros, comportamiento adictivo, propiedad intelectual, ergonomía, privacidad en línea, depredadores y protección de virus. 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.

Contenido

Etiqueta de la Red

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, como “emoticones” y escribe con letras mayúsculas, para comunicar sus emociones.
- 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.
- La comunicación en línea nunca debe ser usada para hacerle daño las otras al difundir rumores o decir cosas malas. Su hijo(a) nunca debe escribir algo que él o ella no dirían a alguien en persona. Su hijo debe decirle a usted o a un maestro cuando alguien está tratando de hacerle daño a alguien más.
- Sólo envíe o publique algo que un padre o maestro 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:

- 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, como “emoticones” y escribe con letras mayúsculas, para comunicar sus emociones.
- 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.
- La comunicación en línea nunca debe ser usada para hacerle daño las otras al difundir rumores o decir cosas malas. Su hijo(a) nunca debe escribir algo que él o ella no dirían a alguien en persona. Su hijo debe decirle a usted o a un maestro cuando alguien está tratando de hacerle daño a alguien más.
- Sólo envíe o publique algo que un padre o maestro 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.

Seguridad del Teléfono Celular

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 envio de mensajes de texto a través un celular. Los niños deben saber cuál es el uso apropiado y seguro de un teléfono celular.

Lo que su hijo(a) debe saber:

- No publique números de teléfono en línea, o puede hacer vulnerable al acoso cibernéntico, a criminales que quieren conocerlo en persona y a estafas o scams.
- Usted nunca puede estar 100 por ciento seguro de que la persona que está enviando el mensaje de texto sea la dueña del teléfono. El teléfono puede haber sido robado, por lo tanto:
    - No envie información personal a través de un mensaje de texto (acerca de sí mismo, a sí misma, o a otros)
    - Nunca envie una contraseña o número de identificación personal a un amigo
    - Si alguien le envía un mensaje de texto para verse, aunque la persona sea un amigo conocido, le debe llamar para confirmar
    - Nunca deje que alguien desconocido use su teléfono celular.
    - Si alguien que usted conoce necesita usar el teléfono para una emergencia o razón importante (tal como llamar a un padre) tenga cuidado y observe cuidadosamente lo que hace la otra persona, para asegurarse de que él o ella no le suplante.
    - 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.
    - Solamente envie textos o responda a la gente que usted conoce. Si el número es desconocido, ignore el mensaje de texto.
- Nunca trate de lastimar a alguien o ayudar a alguien a lastimar a alguien más enviándole mensajes de texto o fotos.
- Siempre piense en cómo se sentiría alguien antes de enviarle un texto. Nunca mande un texto diciendo lo que él o ella no diría en persona. Si usted está enojado, espere antes de enviar un texto.
- Si alguien le manda un mensaje ofensivo o dañino, no lo conteste y enseñeselo a un maestro antes de borrarlo.
- 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.

Seguridad General para el uso del Teléfono

- Nunca envíe un mensaje de texto o hable por el celular mientras maneja.
- Envío excesivo de mensajes de texto puede causar tendinitis de adolescentes, la cual es el principio del síndrome del túnel carpiano.

Consejos para los padres:

- Use un contrato, como el “Contrato de mensajes de texto” en 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 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.
- 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.

Filtros

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. 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.

Opciones para Herramientas de Filtros:

- Bloquear a las personas para evitar que vean material sexualmente explicito en la Web. Pero tenga cuidado, ningún filtro es perfecto.
- Permitir a los padres y cuidadores monitorear actividades en línea.
- Permitir a los padres bloquear horas del día cuando una persona puede o no conectarse a la Internet.
- Prevenir información personal (como nombre, dirección de su casa etc) que sea publicada o mandada por correo electrónico.
- 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.

Comportamiento Adictivo

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.
- Descuida su espacio o aseo personal.

Consejos para los padres:

- Considere todos los factores antes de calificar a su hijo de tener comportamiento adictivo.
- 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.
- 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.

Propiedad Intelectual

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 se pueden encontrar con propiedad intelectual, frecuentemente en la forma de música, películas, videos o programas de TV con derechos de autor.

Lo que su hijo(a) debe saber:

- 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, 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 y para el malware y los programas de “spyware.”

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 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.
- Buscar para archivos de música (MP3s) y no videos archivos o imágenes.
- Asegúrese de que tenga instalado y actualizado software de anti-virus y firewalls.

Ergonomía

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.

Lo que su hijo(a) debe saber:

- 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 y el síndrome del túnel carpiano.

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).

Privacidad en línea

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 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 obtienen acceso a números de tarjetas de crédito y pueden hacer compras y arruinar el crédito de las personas por años.
- Robo de Número de Seguro – Los criminales acceden los números de seguro social y usar los números para crear una nueva identidad o solicitar crédito. Esto podría dañar el crédito por años.
- 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.

Lo que su hijo(a) debe saber:

- El proteger la identidad de los miembros de su familia es una responsabilidad compartida de todos los miembros de la familia.
- No ponga su numero de seguro social en línea.
- Las contraseñas débiles pueden conducir a que tu avatar sea robado o hurtado en sitios de juegos en línea.
- Nunca use 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.
- No dé 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.
- Algunos sitios son seguros, pero otros no. Siempre revise 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
- 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.
- Asegúrese que los ajustes de privacidad de su hijo(a) para sitios de redes sociales estén puestos para que sólo sus amigos puedan ver el perfil de su hijo(a). Revise los ajustes 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.

Depredadores

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. 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.

De acuerdo al Centro de reporte de seguridad en Internet Berkman, basado sobre la investigación hecha por Wolak, Finkelhor, Mitchell y 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.Normal text for paragraph

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.)
- Hable con su hijo acerca de quién 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.

Protección de Virus

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 de aplicaciones intrusivas:

- Virus – Un virus es una pieza de software que se basa en un programa real.
- 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.
- 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.
- 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.

Consejos para los padres:

- 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.
- 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.