ENOUGH·IS·ENOUGH
Making the Internet Safer for Children and Families

DIRECTRICES DE REGLAS Y HERRAMIENTAS PARA LA SEGURIDAD EN EL INTERNET

Poner en práctica reglas de seguridad y herramientas de "software" (inglés por paquete soporte de computadora) para proteger a los niños cuando están "online" (inglés por: en línea, conectado con la computadora). Prestar atención en lo positivo del uso de la Internet mientras le enseñamos a los niños sobre los peligros de la Internet y a como escoger sabiamente cuando están en línea.

Reglas: Medidas no-técnicas

Mientras la tecnología continúa evolucionando, es muy fácil sentir que nos quedamos atrás. Siga estas medidas no-técnicas para ayudarlo a usted a llegar a ser un experto cibernético, un "virtual parent" (inglés por: padre verdadero). Mientras usted se educa acerca de los beneficios y riesgos del Internet, y llega a ser más activo en la vida de sus hijos cuando están en línea, sus acciones y creencias van a establecer un precedente para las acciones de sus hijos cuando están en línea. Enseñe a sus hijos que la diferencia entre lo bueno y lo malo es la misma en el Internet que en la vida real.

*Establezca un diálogo continuo y mantenga las líneas de comunicación abiertas: *Mantenga las líneas de comunicación abiertas: Pase tiempo en el Internet junto con sus hijos y cree una atmósfera de confianza. Anime a sus hijos a elegir bien y suavice sus reacciones cuando ellos se tropiezan con situaciones peligrosas.

- *Los adolescentes cuyos padres les han hablado mucho acerca de la seguridad cuando están en línea, son menos propensos a considerar el encontrarse cara a cara con alguien que ellos han conocido a través de la Internet (12 por ciento versus 20 por ciento).1*

Supervise el uso de todos los dispositivos permitidos del Internet en la computadora: Mantenga la computadora de sus hijos en un área abierta de su casa y controle otros puntos de acceso a la Internet incluyendo el teléfono celular de sus hijos, el iPhone, el mecanismo de música portátil y el PDA.

- *Los padres dicen que ellos pueden vigilar donde entran sus hijos adolescentes en línea si la computadora está en un área publica de la casa.2*

Enseñe a sus hijos como proteger la información personal puesta cuando están en línea y a seguir las mismas reglas con respecto a la información personal de otros: Recuérdele a sus hijos que piensen antes de poner información cuando están en línea: no se puede regresar nada una vez que se pone en línea. Nada es realmente privado en la Internet y toda la información enviada o puesta en línea, es pública o se puede hacer pública.

Advierta a sus hijos acerca de poner información en línea:
Información personal o para ponerse en contacto: El nombre, dirección, número de teléfono, contraseñas e información de identidad financiera debe ser proporcionada solamente en un sitio asegurado y bajo supervisión paterna. *Información personal* íntima: Información privada, personal y sensible (tales como un diario del adolescente) no debería ser puesto online en lo absoluto y si se hace, debería ser compartido solamente a través de un correo electrónico privado con un amigo personal de confianza.

Información dañina para la reputación o imágenes: Fotos explícitas o provocativas, etc. nunca deberían ser puestas en línea o enviadas.

Información acerca de eventos: Enseñe a sus hijos a evitar poner información en línea acerca de fiestas, eventos o actividades donde un predador o abusador puede encontrarla.

- *Los adolescentes cuyos padres han hablado bastante con ellos acerca de la seguridad en el Internet se preocupan más de los riesgos de compartir información personal en línea. Por ejemplo, un 65 por ciento de adolescentes cuyos padres no les han hablado de la seguridad cuando están en línea, ponen información acerca de donde ellos viven, comparados con un 48 por ciento de adolescentes cuyos padres están más envueltos con ellos.3*

Esté alerta de que sus hijos usen escenarios de privacidad para restringir acceso y limitación a quienes puedan mirar sus perfiles en línea: Sitios de conección social en la red proveen una gran variedad de escenarios de privacidad que limita quien pueda ver el perfil del niño. Al usar estas herramientas de privacidad, los padres y guardianes están capacitados para aprobar qué amigos de la escuela, clubes, equipos y grupos comunitarios pueden mirar el perfil del niño u obstruir individuos desconocidos que puedan tener acceso a la información del niño. En la mayoría de los escenarios sociales de los sitios de la red, usted puede tener acceso y cambiar los escenarios de privacidad de sus hijos apretando el ratón de la computadora en "account settings" (inglés por escenarios o aplicaciones de la cuenta). Recuerde que nadie puede detectar a un predador disfrazado.

Inspeccione con regularidad las comunidades en línea que sus hijos usen, tales como escenarios sociales y sitios de juegos, para ver que información ellos están poniendo en línea: Trate de asegurarse que usted, como padre, esté añadido a "la lista de amigos" de sus hijos porque si sus "profiles" (inglés por perfiles) están asignados a "privados" (como debería de ser) usted no podrá ser capaz de mirar ninguna de la información de sus hijos. Si usted no está seguro si su hijo tiene un perfil en la computadora, conduzca una investigación simple en línea a través del sitio en cuestión o escriba en el ordenador el nombre de su hijo en un mecanismo de búsqueda (ejemplo: Google). Esté conciente no solamente de lo que su hijo está poniendo en línea, sino también acerca de lo que otros niños están poniendo sobre sus hijos. Antes de permitirles a sus hijos usar sitios de escenarios sociales en la Internet, EIE anima a los padres que se familiaricen ellos mismos con el contenido del sitio y revisen minuciosamente las practicas de seguridad y herramientas de privacidad disponibles a través de los escenarios sociales y otras comunidades de la red.

- *Una mayoría de adolescentes (58 por ciento) no piensa que poner fotos en línea u otra información personal es arriesgado.5*

Supervise los tipos de fotos y videos que sus hijos ponen en línea y a través de sus dispositivos móviles: Las fotos y los videos pueden ser copiados instantáneamente en sitios tales como "YouTube" y "Facebook" (sitios sociales en la red) desde cualquier plataforma con acceso a la Internet, incluyendo el teléfono celular, cámara de Web, PDA, y dispositivos de juegos. Estas imágenes pueden hacer su hijo vulnerable a predadores de la red, a abusadores cibernéticos y a extraños, o pueden conducir a dañar la reputación de su hijo. Mantenga inspección con la escuela de su hijo para asegurarse que los proyectos, artes o fotos puestos en el sitio de la red de la escuela son solo accesibles a través de contraseñas (o a través de la red de la escuela) y no contienen ninguna información identificable. Los niños mas pequeños no deberían poner, hacer texto o enviar fotos o videos en línea.

- *Los adolescentes están listos para poner información personal en línea. Un sesenta y cuatro por ciento ponen fotos o videos de ellos mismos, mientras más de la mitad (58 por ciento) ponen información acerca de donde viven. Las muchachas tienden a ser mas arriesgadas que los muchachos en términos de poner fotos personales o videos de ella mismas en línea (70 por ciento versus 58 por ciento).6*

Desanime el uso de cámaras de Web y dispositivos de video portátil: Muchas computadoras, teléfonos celulares y otros dispositivos portátiles vienen ahora con cámaras de Web incorporadas y dispositivos de video, pero los videos y las cámaras de Web deberían solo ser usadas bajo supervisión o no usarlas del todo. Los videos deberían enviarse solamente a amigos y familia en los cuales confiamos. Nunca permita que sus hijos usen cámaras de Web u otros dispositivos de videos en sus habitaciones o en otras áreas privadas.

- *Un cuatro por ciento de la juventud que usaron la Internet en el 2005 dijeron que solicitantes en línea les pidieron fotos explícitas de ellos al desnudo o con contenidos sexuales.7*

Conozcan las actividades y amigos de sus hijos en línea: Esté familiarizado con cada contraseña, nombre de pantallas y todas las informaciones de cuenta, y hágalos que les provean las identidades de cada persona en sus listas de colegas o de cualquier persona que ellos se han hecho amigos en los escenarios sociales o sitios de juegos. Alerte a sus hijos acerca de comunicarse solamente en línea con personas que ellos conocen personalmente y que han sido aprobados por usted. Recuérdeles a sus hijos que la gente que ellos conocen en línea puede no ser lo que ellos dicen que son.

- *Casi uno de cada ocho juveniles de edad 8-18 ha descubierto que alguien con quien ellos se estaban comunicando en línea era un adulto pretendiendo ser más joven.8*

Instruya a sus hijos a evitar encontrarse cara-a-cara con alguien que ellos solamente han conocido en línea o a través de sus dispositivos portátiles: "Amigos" en línea y en dispositivos portátiles pueden no ser quienes ellos dicen

que son. Los niños también deberían ser informados de venir en busca de usted si alguien los hace sentir con miedo, incómodos, confundidos, o les piden información personal o identificable o les sugiere encontrarse con ellos personalmente.

- *Un 16 por ciento de adolescentes dicen que ellos han considerado encontrarse cara-a-cara con alguien que han conocido solamente en línea, y un 8 por ciento de los adolescentes dicen que ellos actualmente se han encontrado personalmente con alguien que han conocido a través de la Internet.9*

Enséñele a sus niños como responderle a los abusadores cibernéticos: Los niños no tienen que aceptar ninguna actividad en línea de alguien que trate de intimidarlos, amenazarlos, engañarlos o dañarlos en línea, a ellos o a alguien más. Esté alerta de señales de avisos, incluyendo el desgano de sus hijos a usar el Internet; esté también alerta de los cambios de comportamiento y estado de ánimo de sus hijos. Reporte cualquier correo electrónico, un "Chat" (inglés por charla), o una comunicación que sea ofensiva o peligrosa a las autoridades locales. No borre la evidencia. Recuérdele a su hijo de la Regla de Oro: "Trata a los demás como quisieras que te trataran a tí."

- *En general, un 19 por ciento de los adolescentes reportan que ellos han sido acosados o abusados en línea, y el índice de acoso en línea es más alto (23 por ciento) entre los adolescentes de 16 y 17 años de edad. Las muchachas tienen mas probabilidad de ser acosadas o abusadas que los muchachos (21 por ciento versus 17 por ciento).10*

Establezca un pacto con sus hijos acerca del uso de la Internet en la casa y fuera de la casa (vea las reglas y herramientas del Juramento Juvenil). Recuérdeles que las reglas de buen comportamiento no cambian simplemente porque ellos están usando la computadora o su teléfono celular. Ponga el pacto cerca de la computadora. Esté listo a firmar un juramento como padre también.

- *Un 69 por ciento de adolescentes reciben mensajes personales en línea regularmente de personas que ellos no conocen y la mayoría de ellos no le hablan de ésto a un adulto de confianza.11*

Herramientas: Medidas Técnicas.

Además de las reglas de seguridad, el proteger a los hijos cuando están en línea requiere el uso de "software" (ingles por herramientas o paquetes de computadora), mejor conocidos como paquetes de computadoras de controles para padres. El paquete de computadora de controles para padres ayuda a prevenir contenidos censurables y personas peligrosas a alcanzar acceso a su hijo. Un amplio sitio de "Parental Control tools" (inglés por herramientas de control para padres) debería incluir filtros personalizados, paquetes de computadora para monitorear o supervisar, control para manejar el tiempo, y controles para IM y "Chat" (charla). Los controles para padres deberían ser utilizados en todos los dispositivos permitidos del Internet (computadora de mesa, computadora portátil, y dispositivos de juegos y portátiles). Sin embargo, estos recursos no son un substituto sobre la supervisión de los padres.

Aplique filtros para la edad apropiada: Los filtros obstruyen categorías inapropiadas de sitios de la red que su hijo pueda ver. Las contraseñas de los escenarios son protegidos. Recuerde que ningún filtro es un substituto sobre la supervisión de los padres y los filtros puede que no sean un obstáculo para un niño determinado a sobrepasarlos o deshabilitarlos y lograr acceso a un contenido inadecuado. También, aplique los filtros para obstruir acceso a la red del mismo grupo social (P2P), que permiten a los que lo usan a conectarse directamente con la computadora de cada uno de ellos para recuperar e intercambiar archivos, sin un "Server" (inglés por servidor) y el cual contiene una cantidad tremenda de pornografía y pornografía de niños.

- *Un tercio de los muchachos que usan la Internet entre los 10 y 17 años de edad fueron expuestos a material sexual indeseado y más de un tres cuarto de pornografía indeseada (79 por ciento) y esto pasó estando en la casa.12*

Considere usar un paquete de computadora para monitorear o supervisar, especialmente si usted presiente que su hijo está en riesgo: El paquete de computadora para monitorear, o el dispositivo para capturar el teclado, pueden proveer un registro completo de donde su hijo va cuando está en línea, supervisa las comunicaciones que entran y salen, e identifica los colegas de su hijo en línea. Otras herramientas más robustas para supervisar dejan que los padres puedan ver cada red del Web que los hijos visitan, ver cada correo electrónico o mensajes instantáneos que ellos envían y reciben, y hasta pueden registrar cada palabra que ellos envían en mecanografía. Muchas herramientas de monitorear pueden enviar a los padres un reporte periódico que sumariza el uso que sus hijos han hecho de la Internet y sus

comunicaciones. Estos programas autorizan a los padres y guardianes a aplicar límites a sus hijos en línea. Los padres deberían decirles a sus hijos que se les está supervisando a menos que el padre sospeche que sus hijos están envueltos en un comportamiento riesgoso, en tal caso, puede ser mejor mostrarse más cauteloso.

- *Más de un tercio de muchachos de 16 y 17 años de edad que fueron encuestados dijeron que ellos habían visitado intencionalmente sitios de índice tipo X en el último año. Entre las muchachas de la misma edad, un 8 por ciento lo había hecho.13*

Supervise periódicamente la actividad de su hijo en línea viendo la historia del navegador de la red: Manténgase alerta de sitios que parecen inadecuados (¡aunque no todos los sitios inadecuados tienen un nombre inadecuado!). Si usted nota que la historia ha sido limpiada o destruida, tenga una discusión con su hijo acerca de los sitios que él o ella ha visitado. Si usted está preocupado acerca de la actividad de su hijo en línea, usted podría instalar un paquete de computadora para monitorear o supervisar.

- *Un 65 por ciento de todos los padres y un 64 por ciento de todos los adolescentes dicen que los adolescentes hacen cosas online que a ellos no les gustaría que sus padres supieran*.

Aplique un tiempo limitado: Un tiempo excesivo en línea, especialmente en la noche, pude indicar un problema. Recuérdele a su hijo que el uso de la Internet es un privilegio, no un derecho. Si es necesario, utilice paquete de computadora con herramientas de tiempo limitado, lo cual permite que los padres administren la cantidad de tiempo y las veces durante el día que su hijo tiene permiso para estar en línea.

Considere rechazar acceso a "Chat rooms" (inglés por cuartos de charla): Reconozca que los cuartos de charla hoy en día son el patio de recreo de los predadores sexuales.

Es imposible que un padre, un niño, un monitor de cuarto de charlas o una herramienta de tecnología puedan reconocer un predador anónimo disfrazado.

Un 37 por ciento de incidentes donde hay solicitación sexual ocurre mientras un joven está en los cuartos de charla. 15

Rechace el acceso a cuartos de charla y solo permita audio vivo con mucha precaución: Los cuartos de charla son hoy en día el patio de recreo de los predadores sexuales; estos permiten una comunicación directa e inmediata entre los participantes. Muchos de ellos son dirigidos hacia los adolescentes y se conocen por conversaciones sexuales explicitas y lenguaje obsceno, promoviendo una atmósfera en la cual pueden atraer pervertidores de menores. Los cuartos de charla también permiten a los que los usan a que se comuniquen vía cámaras de computadora y charla de audio.

Muchos programas de juego también vienen equipados con capacidad para charla de audio vivo a través de la cual los individuos pueden alterar el sonido de sus voces. Solamente los adolescentes maduros deberían ser permitidos a usar charla de audio vivo. Recuérdele a su hijo de solo relacionarse con individuos que ellos conocen fuera de los servicios de cuando están en línea. Es imposible que un padre, un niño, un monitor de cuarto de charla, o cualquier herramienta de tecnología puedan reconocer un predador anónimo disfrazado.

La mayoría de los incidentes de solicitaciones sexuales (79 por ciento) pasa en las computadoras de la casa, comenzando con preguntas personales acerca de la apariencia física del adolescente, su experiencia sexual, y con proposiciones para "cybersex" (inglés por sexo cibernético). Un 37 por ciento de incidentes de solicitación sexual ocurre mientras el joven está en cuartos de charla, y muchos ocurren en charla en vivo o en sesiones de mensajes instantáneos.

Limite los contactos de su hijo "Instant Messaging" (inglés por mensajes instantáneos) a una lista de amigos aprobados por usted: Si usted decide permitir que su hijo use mensajes instantáneos, obstruya cualquier comunicación de personas que no estén en la lista pre-aprobada por usted. Paquetes de computadora robustas para el control de padres, pueden prevenir que su hijo añada alguien en la lista a menos que usted lo haya aprobado. Sin embargo, algunos muchachos son capaces de sobrepasa los controles de los padres, así que revise la lista de los amigos regularmente para que esté seguro de que no ha sido alterada.

Esté alerta de que muchas comunidades en línea, tales como red sociales y sitios de juegos tienen ahora mensajes instantáneos y características de charla, y no todos los paquetes de computadora para el control de los padres proveen suficiente amparo sobre estas nuevas plataformas de charla.

Use mecanismos de seguridad de búsqueda: Aunque los mecanismos de búsqueda ayudan a los muchachos a encontrar sitios de la red que son de diversión e información educacional, también pueden ser una forma eficiente de abrirles paso a la pornografía y a otros contenidos inapropiados. Los mayores mecanismos de búsqueda han abordado esta necesidad creando zonas de seguridad para niños. Algunos dan la opción de controles para padres o búsqueda seguras. Consulte la información en su ISP y en la página de aplicaciones del mecanismo de búsqueda para el proveedor para que esté seguro que la opción de búsqueda de seguridad está conectada.

Active la protección ciber-seguridad para la familia: Además de activar los controles para padres, ponga al día el sistema operativo regularmente e instale "Firewall" (ingles por pared contra fuegos o intrusos) y lo último en paquetes de computadora en contra de virus y en contra de espías. Al instante que una computadora es conectada con el Internet o en una conección "siempre puesta," los piratas y ladrones pueden atentar el lograr acceso a la información personal y financiera de la familia. Con su computadora asegurada, usted puede ayudar a protegerse de estos intrusos de la Internet y los programas maliciosos que pueden infiltrarse en su computadora.

Utilice los controles de los padres en el teléfono celular y dispositivos portátiles de su hijo: Todos los portadores mayores de teléfonos celulares ofrecen niveles de control para padres, incluyendo la habilidad de establecer filtros de contenido, destruir o limitar el acceso a la Internet en teléfonos habilitados con acceso a la red. Los controles portátiles también pueden permitirles a los padres a incapacitar, limitar o supervisar los textos de los muchachos, las películas y los mensajes de video.

- *En una encuesta reciente de la Campaña Nacional para Prevenir Embarazos No-Planeados en los Adolescentes, uno de cada cinco adolescentes reportó que ellos habían enviado o puesto en línea, películas de video de ellos desnudos o semi-desnudos.*

Reporte cualquier contenido o actividad que usted sospeche sea ilegal o criminal a las autoridades locales y al Centro Nacional de Niños Desaparecidos y Explotados al http://www.cybertipline.com o al 1-800-843-5678.