Seguridad de Internet

Por: Lucinda Thelen M.Ed., CAPE

Los niños usan Internet para:

- hacer su tarea,
- jugar juegos
- socializar con sus compañeros.

Beneficios:

- apoyar el aprendizaje y la interacción social.
- diseño accesible y lenguaje simplificado,
- clips de vídeo disponibles al instante.
- oportunidades para aprender a través de la repetición
    - más fácil que la comunicación cara a cara.o El uso de emoticonos consistentes y fácilmente reconocibles reemplaza la necesidad de descifrar el lenguaje corporal, las expresiones faciales y el tono vocal de las personas que pueden ser problemáticos en las comunicaciones personales.
    - Permite más tiempo para responder

Si bien el uso de Internet tiene muchos beneficios, también existen riesgos y, con un fácil acceso a Internet, deben aprender sobre estos riesgos y cómo protegerse.

Riesgos:

- Acoso cibernético
    - El ciberacoso es el uso de la tecnología para burlarse, humillar, amenazar y/o acosar a alguien.
- Geolocalización
    - Averiguar quién y dónde estás
- Contenido inapropiado
    - Violencia, pornografía, comportamiento ilegal y discurso de odio
- Información falsa
    - Internet permite que cualquiera, en cualquier lugar, publique cualquier cosa en cualquier lugar.
- Sexting y preparación
    - Sexting es el envío o distribución de imágenes desnudas o parcialmente desnudas
    - Preparar a alguien para que sea un objetivo sexual
- Virus y malware
    - Programas que dañan o roban datos
- El robo de identidad
    - Se adquiere suficiente información personal para que otro individuo se haga pasar por usted (financiero y de reputación)
- Huella digital
    - La información que dejas en Internet (fotos, mensajes, videos, textos) puede perseguirte para siempre
- Salud
    - Sedentario (peso, túnel carpiano, postura), visión, adicción, problemas de sueño,

Todos los niños son vulnerables en línea, pero algunos de nuestros niños pueden tener dificultades para reconocer amenazas y comportamientos amenazantes. Como padre, usted es la primera línea de defensa, así que aquí hay algunas pautas generals

Haga que su red doméstica sea segura

- Manténgalo público: mantenga las computadoras/tabletas/teléfonos en un lugar compartido donde pueda monitorear el comportamiento en línea
- Filtrar contenido: instale filtros (búsqueda segura de Google) y configure controles parentales
    - http://www.toptenreviews.com/software/security/best-internet-filter-software/
    - **https://www.howtogeek.com/167545/4-ways-to-set-up-parental-controls-on-your-home-network/**
- Aumente la seguridad: use protección antivirus y firewalls actualizados
- Use navegadores aptos para niños
    - **https://www.commonsensemedia.org/lists/kid-safe-browsers-and-search-sites#**

Enseñar el comportamiento en línea

- Establezca reglas básicas: identifique qué está bien hacer en línea y qué no.
    - Enfoque de EQUIPO: hablar, explorar, acordar, administrar
    - Lista de contratos o reglas
    - Seguimiento
- Intercambio de información: qué es seguro y qué no lo es
    - No compartir lista
    - Configurar la protección con contraseña
- Netiqueta-
    - Sin rudeza o mezquindad (todo en mayúsculas, insultos, reenvío de información)
- Asuntos legales
    - Su hijo también puede ser acosador cibernético y publicar mensajes e imágenes inapropiados
    - Enséñeles qué es ilegal, especialmente cuando son mayores de 18 años, y qué consecuencias puede tener.
- Recursos y soporte
    - **http://www.netsmartz.org/SpecialNeeds** (también en español)
    - Déles un salvavidas: mantenga la comunicación abierta
    - Juego de roles y práctica de respuestas a posibles amenazas.
    - Google: Sea increíble en Internet https://beinternetawesome.withgoogle.com/
    - Ciudadanía digital Brainpop https://www.brainpop.com/digitalcitizenship/
    - Connect Safely - http://www.connectsafely.org/ Brinda consejos en línea para padres sobre tecnología y cómo usarla de manera segura. Particularmente útil es la guía para padres descargable de Facebook y Snapchat.
- Información falsa
    - El hecho de que esté en Internet no significa que sea cierto
    - Esté atento al "contenido patrocinado"
    - Mire URL- .co en lugar de .com o errores ortográficos
    - Verifique la fuente (sección acerca de nosotros)

        - ¡Compruebe dos y tres veces los hechos!
- sitios de verificación de hechos y sesgos
    - Snopes. Este sitio web independiente y no partidista dirigido por el investigador y escritor profesional David Mikkelson investiga leyendas urbanas y otros rumores. A menudo es el primero en aclarar los hechos sobre afirmaciones de noticias falsas salvajes.
    - https://smhoaxslayer.com/ otro sitio web creíble conocido por desacreditar historias falsas, noticias falsas, rumores virales de Internet y leyendas urbanas. En realidad, también hay una sección dedicada en el sitio que enumera muchos correos electrónicos extraños y difíciles de creer e historias virales que en realidad son ciertas para variar.
    - Politifact. Este sitio web ganador del premio Pulitzer califica la precisión de las afirmaciones de los funcionarios electos. Dirigido por editores y reporteros del periódico independiente Tampa Bay Times, Politicfact presenta el Truth-O-Meter que califica las declaraciones como "Verdaderas", "En su mayoría verdaderas", "Medio verdaderas", "Falsas" y "Pantalones en llamas".

Ahora revisemos los riesgos nuevamente con más detalle:

Ciberacoso (Ciberacoso es el uso de la tecnología para burlarse, humillar, amenazar y/o acosar a alguien)

- Puede realizarse a través de mensajes de texto o redes sociales. Los acosadores cibernéticos pueden enviar comentarios crueles, publicar fotos vergonzosas o compartir información privada sobre alguien para humillarlo o burlarse de él en línea. Incluso si su hijo no está siendo acosado cibernéticamente, recuérdele que es trabajo de todos prevenir el acoso y anímelo a tomar una posición.
- Señales de estar siendo acosado cibernéticamente
    - Evita usar internet
    - Parece estresado o ansioso cuando recibe correos electrónicos o mensajes
    - Se aleja de familiares y amigos.
    - Se resiste a asistir a funciones familiares o escolares.
    - Muestra signos de depresión, baja autoestima o miedo
    - Calificaciones decrecientes
    - Problemas para comer o dormir
    - Caso grave: considerando el suicidio
- Enséñele a su hijo estas respuestas
    - No responder a los mensajes
    - Guardar la evidencia
    - Reportarlo
- Si ven a alguien más siendo acosado cibernéticamente
    - No reenvíes mensajes o fotografías embarazosas
    - No comentar publicaciones insultantes o acosadoras.
    - Reportarlo
    - Apoyar a la víctima siendo un buen amigo

Enseñar privacidad (esto aborda el robo de identidad, la geolocalización y la preparación)

- Conectarse a Internet es como salir en Halloween
    - La cara de todos está oculta
    - A menos que conozca el disfraz de su amigo (nombre en línea), no sabe si está hablando con su amigo (John Doe no es John Doe)
    - Cualquier extraño puede hacerse pasar por un amigo y llamar a tu puerta
- No compartas
    - Correo electrónico
    - Nombre completo
    - Ubicación o número de teléfono
    - Nombre de la escuela
    - Contraseñas o cualquier información personal
- Formas en que comparte información sin querer
    - Nombres de usuario
    - Geolocalización
    - Fotos
- Trucos para que compartas
    - Ventanas emergentes
    - Solicitudes de amistad
        - Recordar círculo de amigos
        - Solo dar información al círculo interno
    - Sitios web o enlaces fraudulentos
        - Busca https:// o bloquea en la ventana del navegador
        - Utilice la búsqueda segura de Google
        - Conoce tu dominio
            - .edu- escuela, colegio o universidad
            - .gov- agencia gubernamental
            - .com: negocio comercial (asegúrese de que sea legítimo)
            - .net-red
            - .org- organización de defense
- Respuestas de los padres
    - Verifique los comentarios y las imágenes en busca de información personal y contenido inapropiado, enséñelos y luego elimínelos.
    - Mirar las listas de contactos. Si no los conoce, verifique lo que están compartiendo para asegurarse de que sea apropiado.
    - Comprobar la configuración de privacidad

Contenido inapropiado

- Establezca la regla: si ve algo que lo hace sentir incómodo, triste, asustado o confundido
    - Presiona el botón Atrás
    - Apagar la pantalla
    - Dile a un padre o figura de autoridad

- Acciones de los padres
    - Verificar el historial del navegador
    - Hablar sobre lo que están haciendo
    - Mantenlo visible
- Trolls: crean problemas a propósito
    - No responda (No los alimente)

Sexteo y Grooming

- Los mensajes, las salas de chat y las redes sociales alimentan a los perpetradores.
    - La intención puede ser avergonzar, humillar, intimidar o agredir
    - Si la persona no es un amigo del círculo cercano, no proporcione información personal, sin importar cuán "amigable" sea.
    - No hay reuniones cara a cara
- Esté atento a los cambios
    - Aumentar el tiempo en línea
    - Enojarse cuando no está permitido en el dispositivo
    - Tomar medidas adicionales para ocultar lo que están haciendo en línea
    - Recibir regalos o fotos de personas desconocidas
- Los espacios sociales (Facebook, salas de chat, mensajes de texto) son como una casa
    - ¿Abres la puerta a extraños? No, entonces, ¿por qué hacer amigos con ellos o incluso hacer pública su dirección?
    - ¿A quién dejas entrar en tu casa? Su página de redes sociales o aplicaciones son su sala de estar, eso es para amigos y familiares.
    - Dormitorio: este es un lugar privado: muy pocas personas deben ingresar. Esto significa compartir sus sentimientos, deseos, necesidades y detalles personales.
    - Baño: ¡esto está fuera del alcance de todos menos de usted! Nadie debe pedir información o imágenes sobre su cuerpo.
- Respuestas de los padres
    - Escuche activamente, no parezca sorprendido o incrédulo.
    - Mantenga la calma.
    - Tómese en serio lo que le digan.
    - No pida detalles.
    - Asegúreles que están haciendo lo correcto.
    - No prometas guardar secretos.
    - Dígales que tendrá que compartir esta información.
    - Explique lo que sucederá a continuación.
    - Familiarícese con sus procedimientos de protección infantil.
    - Registre la información lo más rápido posible: hechos, no opiniones.
    - Firme y feche todo lo que registre.
    - Obtenga apoyo para usted mismo.

Huella digital (el retrato de quién eres en línea)

- Lo que se comparte se comparte para siempre (fotos, mensajes, videos, textos)
    - Sus llamadas de Skype, comentarios en las redes sociales, uso de aplicaciones y correos electrónicos pueden ser vistos por otros o rastreados en una base de datos
    - Esta información se puede compartir con otros, ser analizada por posibles empleadores y utilizada para dañarlo.
- Respuestas de los padres
    - Enséñeles que lo que sea que publiquen o vean no es privado y que deberían estar de acuerdo con que cualquiera lo vea.
    - Pídales que imaginen que lo que escriben o las imágenes que comparten podrían compartirse en cualquier parte del mundo.

Virus o Malware

- Proteja su computadora con protectores de virus o cortafuegos actualizados
- No responda a las ventanas emergentes ni abra los archivos adjuntos
- No haga clic en enlaces que no sabe que están protegidos sin importar de quién provengan
- No responda ni abra correos electrónicos no deseados
- Actualice las aplicaciones para obtener la protección más reciente
- Si se comunica que hay un problema, comuníquese directamente con la empresa

Salud (problemas físicos, trastornos del sueño, visión y adicción)

- Establecer límites de tiempo para dónde, cuándo y la duración del uso del dispositivo
- Establezca pautas claras de uso y sea consistente
- Establecer consecuencias

Información Adicional

- Aplicaciones
    - Información de seguridad en línea: https://www.nspcc.org.uk/keeping-children-safe/online-safety/ Ajustar la configuración de privacidad
- Teléfonos inteligentes/tabletas
    - Los teléfonos zombi cobran vida con Wi-Fi
    - Comprender el sistema de ubicación y deshabilitar para aplicaciones y publicaciones en línea
    - Aprender siglas
    - Controlar el uso nocturne

¿Están listos para un teléfono celular?

- ¿Pueden seguir el ritmo de su ubicación?
- ¿Recuerda cargarlo?
- ¿Pueden evitar dañarlo?
- ¿Respetarán y comprenderán los límites del plan del teléfono?
- ¿Revisarán y responderán a los mensajes?
- ¿Seguirán las reglas para el uso de teléfonos celulares en el hogar, las escuelas y los lugares públicos?
- ¿Entenderán cómo es el acoso y el contacto inapropiado?
- ¿Pueden entender y usar emojis y abreviaturas apropiadamente?

- ¿Usted como padre tiene suficiente tiempo e interés para enseñarle a su hijo a usar su teléfono?

Juegos

- Conocer las características de seguridad
- Mantenga las consolas en un lugar fácil de supervisar
- Establezca reglas sobre cuánto tiempo pueden jugar, qué tipos de juegos pueden jugar y quién más puede participar
- Utilice la Junta de Clasificación de Software de Internet http://www.esrb.org/

Nada importa más que proteger a su hijo, tanto en el ámbito digital como en el mundo real. Use estos consejos y mejores prácticas para crear una experiencia en línea segura y positiva para su hijo.