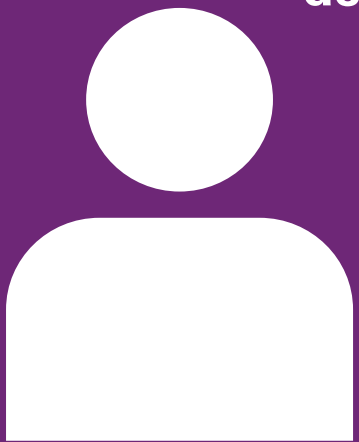
KPMG

Ciber inteligentes

Consejos de ciberseguridad para los más chicos.

7–10 años

La vida durante la pandemia ha sido difícil tanto para los padres y los responsables a cargo de menores como para los propios chicos. Las chicas y los chicos de todas las edades se conectan a sus dispositivos, actualmente, todos los días, para aprender, para jugar o para interactuar con amigos. Este aumento del tiempo frente a las pantallas les suma otra preocupación a los padres y a los responsables de la crianza.Ahora más que nunca ¿cómo pueden los padres y los responsables asegurarse de que los chicos están seguros mientras están conectados y de qué toman decisiones inteligentes?



Hablar acerca de la seguridad informática desde el principio y participar

- Sean honestos, directos y generen confianza, explíquenles por qué es importante tener cuidado mientras están conectados.
- Enséñenles a utilizar contraseñas, a identificar los sitios web seguros, cómo detectar engaños, cuáles son las conductas adecuadas en las interacciones virtuales y muchas otras competencias básicas.
- Asegúrense de preguntarles a los chicos qué hacen cuando están conectados, por ejemplo, que sitios web visitan y con quién hablan.
- Practiquen con el ejemplo y apliquen estos procedimientos cuando Uds. mismos estén conectados

Practicar la ciber inteligencia

Les acercamos estos seis consejos de ciberseguridad para proteger a los chicos.

1. Establecer algunas normas básicas.
Ayuden a moderar el tiempo frente a las pantallas con límites respecto de cuánto tiempo pueden los chicos estar conectados y qué pueden hacer. Se puede restringir el tiempo de conexión que no se relacione con las tareas escolares una vez que las hayan terminado o durante los fines de semana. También es una buena idea ubicar a las computadoras en lugares comunes y monitorear la actividad de los chicos.

2. Restringir el acceso a internet y monitorear las actividades.
No es necesario que sean especialistas en informática para proteger sus computadoras y a sus niños. Las aplicaciones de control para padres y aquellas que se encuentran incorporadas a los dispositivos, computadoras y *routers* de Wi-Fi son muy fáciles de usar. Estos controles les permiten establecer tiempos de acceso, monitorear las actividades en Internet y bloquear algunas categorías de sitios web. Estar al tanto del contenido al que acceden los chicos los ayudará a mantenerlos seguros. Utilicen esta oportunidad para charlar con los chicos acerca de cuáles son las páginas más adecuadas para sus respectivas edades.

3. No brindar información personal.
Recuérdenles a los chicos que no deben brindar información personal, por ejemplo, el nombre completo, la dirección, las contraseñas, la ubicación o el número de teléfono a toda persona que no conozcan, ya sea en las redes sociales o en los juegos en línea. Para mantener la seguridad de la información personal, les pueden decir que utilicen diferentes contraseñas para cada cuenta que tengan en las plataformas en Internet y, luego monitoreen esas cuentas para verificar la actividad.

4. Atención ante el contacto con extraños.
Háblenles de los riesgos de interactuar con extraños, ya sea mediante plataformas de redes sociales, foros de debate o juegos en línea. Insístanles en que nunca queden en encontrarse con alguien fuera de la virtualidad. Si quieren tener una conversión "fuera de línea" con alguna persona, deberán acudir a Uds. para que organicen una forma segura de encontrarse.

5. Pensar antes de postear.
Enséñenles a los chicos a pensar acerca de sus comentarios o de las fotos que pretenden subir a cualquier plataforma en Internet. Explíquenles que una vez que suben el contenido queda en Internet o en el ciberespacio. Esto es especialmente importante, ya que a medida que los chicos crecen y empiezan a buscar trabajo, muchos empleadores hacen una investigación previa de los posibles candidatos en Internet. Hablen con los chicos acerca de las configuraciones de privacidad y aclárenles la diferencia entre salas de chat privadas y públicas o abiertas.

6. Ser amigos, no acosadores.
Hablen con los chicos y enséñenles a denunciar comentarios ofensivos o hirientes inmediatamente. Si sospechan que los están acosando virtualmente, mantengan una comunicación abierta para que ellos sientan que pueden recurrir a Uds. si son objeto de maltrato en las redes. Recuérdenles que deben ser cuidadosos con lo que dicen, envían o postean acerca de alguien más, el *bulling* no intencional sigue siendo *bulling*. La lectura o reenvío de mensajes ofensivos fortalece a los acosadores y lastima a las víctimas aún más.

Online gaming

- Implementar restricciones en el *app store* para evitar que los más pequeños de la familia descarguen aplicativos con calificaciones que no sean para su edad y establecer contraseñas que eviten las compras accidentales de juegos en línea.
- Establecer las expectativas y las normas en relación con los límites de tiempo y los juegos permitidos.
- Limitar los chats a los necesarios para el juego.
- Asegúrense de que los chicos entiendan cuál es la información personal y que no deberían compartirla en un juego en línea o en toda otra interacción virtual en ninguna ocasión.

Redes Sociales

**La mayoría de las redes sociales cuentan con restricciones de edad para crear y usar cuentas. Asegúrense de seguir las pautas en torno a la restricción de edad y de monitorear el uso.*

- Los chicos deben saber que tienen que pensar antes de postear comentarios o fotos y que nunca deben compartir información personal, como, por ejemplo, la edad, la escuela, el domicilio o el nombre completo.
- Sea "amigos" o "seguidores" de sus hijos en las redes de manera de verificar la actividad que se lleva a cabo. No tienen que participar, solamente, ver los perfiles y posteos con la mayor frecuencia posible.
- Lean el apartado sobre lineamientos de redes sociales para padres para saber más acerca de cómo proteger las cuentas de sus hijos en las redes sociales.
- La información que se sube a una red social se guarda y, en general, se comparte por defecto. Asegúrense de que el perfil de sus hijos se encuentre configurado como Privado. Accedan a la configuración y ayúdelos a ajustar los controles por defecto.

Ciberacoso

Comunicación

Hablen con los chicos y enséñenles a:

- Denunciar comentarios ofensivos o hirientes inmediatamente, más allá de que sean ellos o no los objetos de dichos comentarios.
- Presten atención a lo que dicen, envían o postean acerca de alguien más, el *bulling* no intencional sigue siendo *bulling*.

Reconocimiento

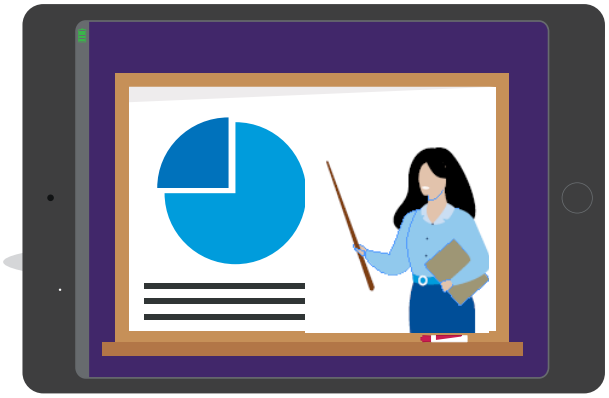
Señales que muestran las víctimas de ciberacoso:

- Enojo repentino, depresión, frustración después de utilizar un dispositivo o abandono de todos los dispositivos.
- Resistencia para ir a la escuela o participar de actividades en equipo.
- Distanciamiento anormal de los amigos más cercanos y de los miembros de la familia.

Acción

Es necesario adoptar las medidas correctas:

- Guardar textos/posteos/correos electrónicos.
- No responder y no borrarlos.
- Denunciar la identificación en línea y bloquear al usuario para evitar futuras interacciones.
- Informar a la escuela o denunciar ante la policía, si fuera necesario.



Aprendizaje a distancia

- Sigan las indicaciones de las escuelas sobre aprendizaje a distancia.
- Preparen a los chicos y diseñen un plan diario.
- Conozcan la tecnología y asegurénse de que los aplicativos de aprendizaje están actualizados.
- Generen un entorno escolar y establezcan un lugar dedicado al espacio de aprendizaje.
- Asegúrense de que los chicos cuenten con todo el material necesario para cumplir las tareas.
- Mantengan la cámara del dispositivo cubierto cuando no lo estén utilizando.
- Ayúdenlos a encontrar su propia motivación.
- Recuerden agendar horas de juego.
- Combinen el tiempo frente a la pantalla con medios de aprendizaje tradicionales, tales como libros de texto y tomar notas.

¿Qué pueden hacer?

Restringir el acceso a internet y monitorear las actividades.

No es necesario que sean especialistas en informática para proteger sus computadoras y a sus niños. Las aplicaciones de control para padres y aquellas que se encuentran incorporadas en los dispositivos, computadoras y routers de Wi-Fi son muy fáciles de usar. Estos controles les permiten establecer tiempos de acceso, monitorear las actividades en Internet y bloquear algunas categorías de sitios web. Estar al tanto del contenido al que acceden los chicos los ayudará a mantenerlos seguros.

Los controles para padres pueden utilizarse para evitar que los chicos accedan a sitios web inadecuados y pueden aplicarse en toda la red o en los dispositivos en particular.

El tiempo programado de Internet puede utilizarse para restringir el acceso a Internet en horarios predeterminados, por ejemplo, después de las tareas o durante los fines de semana.

El registro y monitoreo de la red les permite controlar las actividades de los chicos en Internet y verificar que están usando Internet de manera segura. También, pueden utilizar esta oportunidad para charlar con los chicos acerca de cuáles son las páginas adecuadas para sus respectivas edades.

El antivirus puede servir como la última línea de defensa para proteger la computadora y la información que alberga ante los ataques informáticos (virus) y otros tipos de software malicioso (*malware*).