Common Sense opina sobre la seguridad en línea

¿Cuál es el problema?

La tecnología permite a los niños y adolescentes conectarse fácilmente y compartir cosas con amigos y familiares, no importa donde estén. Pero estas conexiones pueden implicar un enorme costo si los niños y adolescentes no tienen cuidado. Aprender a proteger la información de la identidad personal, crear contraseñas seguras y ser prudente al descargar programas y archivos es muy importante para la seguridad de los niños y la protección de la información almacenada en sus dispositivos digitales. De lo contrario, los niños y adolescentes pueden exponerse y exponer a sus familias a amenazas digitales como virus informáticos, robo de datos e identidad y piratería informática.

Para entender la seguridad y protección digital, tendrá que aprender algunas palabras que quizás no conozca: *phishing (suplantación de la identidad)*, *malware (programas maliciosos)*, *spyware (programas espía)*, *spam (correo publicitario no solicitado)* y sí, hasta *basura*. Todos estos términos se refieren a ávidos programas pequeños que se adjuntan a software que aparenta ser respetable; por ejemplo, un juego para descargar que parece realmente muy bueno, y luego causa estragos una vez instalado en su computadora. Los programas de seguridad pueden ayudar a bloquearlos, pero una de las defensas más importantes contra estas amenazas es enseñar a los niños y adolescentes a tratar sus dispositivos y su información como las cosas verdaderamente valiosas que son.

¿Por qué es un tema importante?

Si los niños y adolescentes no protegen su información personal, existen muchos riesgos potenciales: daños al hardware, robo de identidad o pérdida económica. Pero posiblemente, los niños y adolescentes no se den cuenta de que están poniendo en peligro su información, porque los signos de advertencia no siempre son obvios. Por ejemplo, un amigo puede pedirle la contraseña de la computadora a su hijo para jugar un juego y, luego, puede acceder a la cuenta de correo electrónico privada de su hijo. O bien, su hijo puede usar un programa para compartir archivos que le transmite un virus a su computadora. Es posible que un ladrón, haciéndose pasar por otra persona, pida a los niños de los últimos grados de la escuela primaria que brinden información de identidad personal, por ejemplo, el número telefónico de su casa, su dirección, fecha de nacimiento o su número de seguro social, exponiendo a la familia al riesgo de robo de identidad. Al igual que en la vida real, los niños y adolescentes deben saber a quién le confían la información por Internet.

Common Sense dice

Ayude a su hijo a dominar el arte de la creación de contraseñas. Enséñele a:

- **No usar contraseñas que sean fáciles de adivinar, como su apodo o el nombre de su mascota.**
- **No usar información de identidad privada en la contraseña.** Los ladrones de identidad pueden usar esta información para hacerse pasar por ellos.
- **No usar una palabra del diccionario como contraseña.** Los piratas informáticos usan programas que prueban cada palabra del diccionario para adivinar contraseñas.
- **Usar combinaciones de letras, números y símbolos.** Son más difíciles de decodificar que las palabras regulares porque hay más combinaciones para probar.

Enséñeles a sus hijos a ser prudentes con las cosas que descargan. Dígales que no deben descargar juegos o videos gratuitos a sus computadoras. Estos programas a menudo incluyen programas espía y virus que acabarán con la computadora en reparación y ellos se meterán en un lío. En definitiva, lo que aparentemente es un programa gratuito termina teniendo un costo.

Enseñe a sus hijos a identificar y manejar el spam. Explíqueles que el spam es correo basura que se transmite por Internet. Este tipo de correos no se deben abrir porque, de hacerlo, seguirán recibiendo cada vez más. La mejor estrategia es no abrir correos electrónicos provenientes de direcciones desconocidas.