Educación virtual:

11 maneras de mantener a su hijo seguro en línea

Septiembre de 2020 (Actualizado en abril de 2022)

Consulte nuestra lista de verificación de seguridad en línea para ayudarlo, como padre o tutor, a asegurarse de que su hijo se mantenga seguro mientras aprende en línea.

A menudo, el comienzo de un año escolar significa nuevos lápices afilados, nuevas clases y nuevas rutinas. La pandemia de COVID-19 continúa trayendo nuevas estructuras y procesos de aprendizaje a la educación. Algunos estudiantes obtienen su educación completamente en línea, algunos tendrán una combinación de aprendizaje virtual y en persona, y algunos asistirán físicamente a todas sus clases. No importa qué forma tome la educación de su hijo, es probable que tenga que participar en su educación en línea de alguna manera. Siga estos pasos para mantenerlos seguros.

1. Eliminar los asistentes inteligentes durante el horario escolar

Su asistente inteligente siempre está escuchando por una palabra que lo "despierte", lo que significa que puede escuchar las clases y conversaciones de su hijo con sus amigos. Pídale a su hijo que apague el asistente de voz en su computadora portátil, tableta o teléfono. Si desea eliminar las grabaciones, puede hacerlo en los dispositivos Amazon Echo, Siri de Apple y Google Home.

2. Utilizar un administrador de contraseñas y contraseñas únicas

Su hijo puede usar múltiples servicios en su computadora portátil, tableta o teléfono. Anímelo a usar contraseñas únicas y un administrador de contraseñas. Esto significa que solo deben recordar una contraseña para acceder a todas las demás contraseñas únicas que les permiten acceder a sus cuentas en todos los dispositivos. Usted y su hijo pueden obtener más información sobre los diferentes administradores de contraseñas buscando en línea y leyendo artículos aquí, aquí y aquí.

Las contraseñas no deben ser fáciles de adivinar ni contener información personal, como los nombres de las mascotas. No deberían ser demasiado cortas, ya que eso también puede hacer que los

CC BY-NC-SA 4.0

malhechores las descifren más fácilmente. El uso de la misma contraseña para todos los servicios puede poner la información de su hijo en mayor riesgo de piratería. Es significativamente más fácil para los malhechores acceder a las cuentas cuando todas tienen la misma contraseña. Recuérdele que nunca comparta su contraseña con nadie.

3. Mantener cuentas de correo electrónico principales

Explíquele a su hijo que mantener su cuenta de correo electrónico principal es importante porque muchos servicios usan esa dirección como nombre de usuario de su cuenta, para comunicar restablecimientos de contraseña cuando se olvida o se pierde una contraseña, y para identificarlos. Si su cuenta es pirateada, un malhechor podría usar ese acceso para tomar el control de sus otras cuentas, incluidas las identidades de juegos, e incluso hacerse pasar por ellos en las redes sociales. Utilice una contraseña segura y evite el uso de servicios que eliminan automáticamente las cuentas de correo electrónico después de un período de inactividad. Recuerde cambiar la dirección de correo electrónico de todas las cuentas de su hijo antes de cambiar a una nueva dirección de correo electrónico.

4. Utilizar autenticación de dos factores

Es posible que algunas escuelas ya utilicen la autenticación de dos factores para algunos servicios, pero también puede consultar qué servicios le permiten agregar esta capa adicional de seguridad. Las mejores opciones son las aplicaciones de autenticación y los tokens de autenticación físicos que su hijo puede conectar a su computadora como una llave USB.

5. Buscar servicios con cifrado fuerte

Los distritos escolares a menudo eligen los servicios que se usan para el trabajo escolar, pero usted también puede opinar para asegurarse de que su hijo use otros servicios que ofrezcan un cifrado sólido. Pueden usar servicios de mensajería cifrada de extremo a extremo para comunicarse con sus compañeros de clase. Anímelos a comunicarse solo en grupos cerrados con amigos y a informar cualquier mensaje no deseado. Recuérdeles que lo que publican puede copiarse y reenviarse sin su permiso, o incluso usarse en su contra. Busque en línea para averiguar qué servicios ofrecen cifrado de extremo a extremo.

6. Elegir un navegador y motor de búsqueda que respeten la privacidad

Los niños pueden pasar mucho tiempo navegando por Internet para completar sus proyectos escolares y explorando lo que está disponible en línea a un nivel más personal. Parte de esa búsqueda consiste en descubrir quiénes son, sus intereses y sus valores. El historial de búsqueda de su hijo puede revelar

CC BY-NC-SA 4.0

mucho sobre sus sentimientos, esperanzas y temores más íntimos. Elija un navegador que ayude a protegerlos de los rastreadores y un motor de búsqueda que no rastree su historial de búsqueda.

7. Utilizar una VPN

Una red privada virtual (VPN) puede proteger el uso de Internet de su hijo para que no sea observado por su proveedor de servicios de Internet (ISP) y terceros malintencionados que podrían estar intentando espiar o interceptar el tráfico de Internet. Si su distrito escolar distribuye dispositivos, es posible que ya incluyan VPN. Puede investigar qué tipo de VPN sería mejor para usted y su hijo.

8. Actualizar regularmente el software

Actualizar el software es una manera fácil de garantizar de que la información esté lo más segura posible. Las actualizaciones de software corrigen errores y vulnerabilidades de seguridad y pueden hacer que la información de su hijo esté más segura. Ejecute actualizaciones de software durante las pausas para el almuerzo o cuando vuelva de la escuela.

9. Hacer una copia de seguridad de los archivos

Nadie quiere tener que volver a hacer su tarea. Anime a su hijo a guardar regularmente mientras trabaja en las tareas y a hacer una copia de seguridad en caso de que algo salga mal. Si su hijo o su escuela es víctima de un ataque, un malhechor puede comprometer o bloquear archivos, incluidos documentos escolares importantes, notas de clase y calificaciones. Los distritos escolares pueden ofrecer opciones de copia de seguridad, pero también puede buscar proveedores en la nube y/o dispositivos de almacenamiento externo para asegurarse de que los archivos de su hijo estén seguros. Recuerde buscar una opción de copia de seguridad encriptada y protegida con contraseña.

10. Iniciar una bóveda digital

Nunca es demasiado pronto para alentar a su hijo a armar una bóveda digital segura con documentos e información importantes que pueda necesitar en caso de un desastre natural, una emergencia familiar u otra situación. También es un buen lugar para almacenar copias de certificados y referencias de trabajos extracurriculares. Pregúntele a su hijo si tiene algún recuerdo o archivo que no quiera perder (como novelas gráficas, historias, fotos, videos o arte que haya creado) y guarde una copia digital en su bóveda. Ayúdelo a desarrollar una estrategia para asegurarse de que no “pierda la llave” de la bóveda.

CC BY-NC-SA 4.0

11. Solicitar capacitación en seguridad en línea

Sugiera a la escuela o biblioteca que introduzca capacitación en privacidad y seguridad en línea entre grupos de estudiantes mayores inscritos en ciencias de la computación y estudiantes más jóvenes. No todos los distritos escolares o bibliotecas tendrán los recursos para ofrecer estos servicios, pero alguien dentro de la comunidad puede conocer a alguien que podría ayudar a encontrar los recursos humanos y financieros para hacerlo.

CC BY-NC-SA 4.0