DISTRITO ESCOLAR METROPOLITANO DE CLEVELAND

CMSD ALL
Excellence for ALL
OPPORTUNITY | EQUITY | SUCCESS

Seguridad en Internet:

CONSEJOS PARA PADRES Y REPRESENTANTES

En esta época digital, es fundamental que los estudiantes adquieran habilidades tecnológicas y que tengan acceso a internet. Pero, los dispositivos digitales y redes informáticas presentan riesgos digitales y sociales para ellos y para todos. Los riesgos digitales incluyen software que podría poner a riesgo la seguridad del dispositivo y la información que contiene.

Los riesgos sociales—a veces conocidos por el término "ingeniería social"—ocurren cuando uno cae víctima a una trampa y comparte su información privada y, como consecuencia, pone a riesgo su seguridad personal. Mientras que nadie es 100% seguro cuando trabaja en línea, hay varias formas en las que padres y representantes pueden proteger a sus hijos y reducir bastante estos riesgos. A continuación compartimos unos consejos de seguridad de internet con el fin de asegurar que su hijo y toda la familia tengan una experiencia en línea segura.

Hable con su hijo sobre el uso de internet. Háblele con frecuencia sobre cómo usan internet. Si están acostumbrados y se sienten cómodos hablando con usted sobre internet, no dudarán de informarle si hay un problema.

Establezca límites en el uso de internet.
Es importante establecer normas para sus hijos para que entiendan sus expectativas. Establezca y aclare las normas antes de que ocurra algo malo.

Explique los peligros de las personas desconocidas que podrían contactarlos en línea. Los niños y adolescentes deben comprender que el extraño en línea no es distinto a una persona que llama a su puerta pidiendo que le deje entrar.

Recuérdeles a sus hijos que nunca deberían divulgar información personal como su(s) nombre(s), apellido(s) o teléfono ni tampoco proporcionar la información de otra persona:

- Nunca reunirse en persona con una persona que te haya contactado en línea o que hayas conocido en un chat.
- No revelar tu ubicación actual o adónde piensas ir.
- Si alguien dice o hace cualquier cosa en línea que te hace sentir incómodo, infórmale a tu padre/representante o al maestro. Bloquea a esa persona y no respondes.

Enseñe a sus hijos a mantener la privacidad de su información personal. Nunca es una buena idea postear información personal en línea como teléfonos, direcciones y números de tarjeta de crédito.

Infórmese sobre los riesgos de divulgar información personal en las redes sociales. Los sitios como Facebook permiten que los adultos y niños compartan fotos y videos y conversen con amigos como también con personas desconocidas. Si su hijo comparte algo con sus amigos, es posible que un adulto lo vea y utilice la información para fingir ser estudiante o amigo de un estudiante. Por lo tanto, es importante recalcar la importancia de evitar contacto en línea con personas desconocidas.

Dígale a su hijo que está bien hablar con usted si tiene un problema. Si su hijo se mete en un problema en línea o se siente sospechoso o incómodo debido a algo que ocurrió en línea, déjele saber que usted desea ayudar y apoyarlo.

Tome tiempo para conversar con su hijo sobre seguridad en internet

Salas de chat "Amigos" (Redes sociales)
Gente de cualquier edad puede entrar a una sala chat o contactar a otras personas por una red social. Por lo tanto, para proteger a sus hijos, es importante emplear el mismo nivel de precaución que emplea en el ámbito público. Hable con su hijo sobre los siguientes riesgos: 1) Hay personas que postean perfiles falsos o envían fotos fingiendo ser una persona de su edad para ganar su confianza o 2) te invitan a reunirse en privado.

Ciberacoso
El ciberacoso es bullying que ocurre a través de medios digitales como teléfonos celulares, computadoras y tabletas. Incluye mensajes de texto o en línea en las redes sociales, los sitios de videojuegos o en cualquier lugar donde la gente puede ver, interactuar con o compartir contenido. El ciberacoso incluye el envío, publicación, o compartir contenido negativo, dañino, falso o cruel sobre otra persona. Si observas o te enteras de este tipo de comportamiento, deberías reportarlo a tu padre/representante o maestro, así como reportarías bullying en la escuela.

Fraudes por internet
Nunca hagas clic en enlaces o adjuntos en un email a menos si conoces a la persona que te lo haya enviado y/o estabas esperando el email. Las siguientes trampas son comunes y son diseñados para atraer la atención de estudiantes:

- anuncios y subastas garantizando productos de lujo a precios increíblemente bajos—productos que, una vez pedidos, nunca llegan.
- concursos, becas u ofertas de empleo que requieren el pago de una cuota o un depósito.
- ofertas de servicios gratuitos para teléfonos celulares, cuando, en realidad, incurren una tarifa mensual.

Cómo reportar problemas e inquietudes sobre seguridad en internet

Acceso o exposición a contenido inapropiado

Mientras que el internet es fundamental en esta época digital, también posibilita la exposición a una gran cantidad de contenido. Sea a propósito o no, los niños pueden llegar a observar material inapropiado o hasta obsceno. Hay varios pasos que padres y representantes pueden tomar para avisar a su hijo sobre las consecuencias de acceder contenido inapropiado en línea:

- Dígale a su hijo que salga del internet y reporte el contenido inapropiado que ha aparecido en su dispositivo a su maestro.
- Infórmele a su hijo que los dispositivos del Distrito que están usando mantienen un registro de todos los sitios que hayan accedido.
- Recuerde a su hijo que, si intenta desactivar el sistema de filtrado de contenido, corre el riesgo de la misma consecuencia como si hubiese accedido el contenido inapropiado en la escuela.

Si su hijo siente que podría haber sido víctima de una amenaza en línea, siga los siguientes pasos:

- Llame al Departamento de Tecnología de CMSD al 216.838.0440 para reportar el incidente, amenaza o problema al maestro de su hijo y al director de su escuela.
- Los Departamentos de Ciberseguridad, Gestión de Riesgo y Seguridad y Protección estarán avisados inmediatamente.
- El Departamento de Ciberseguridad y/o Seguridad y Protección se comunicará con el padre/representante para resolver el asunto. Padres/Representantes pueden contactar a la policía, si desean.