Fostering Family

GUÍA DE ESTUDIO DE MEDIOS SOCIALES

Más recursos disponibles en **fosteringfamily.com**

Facebook

Una fuente de noticias es lo primero que ves cuando inicias sesión en Facebook, verás lo que dicen tus amigos, de qué están hablando, imágenes o medios que están compartiendo, verás artículos de noticias, verás anuncios publicitarios. Todo esto se mostrará como una fuente de noticias.

También hay grupos en Facebook. Los grupos pueden ser donde grupos de personas pueden compartir contenido de ideas afines. Verás grupos que compran/venden/intercambian, verás grupos de pasatiempos, política, religión; hay todo tipo de grupos disponibles.

Facebook tiene una aplicación de Messenger. Aquí es donde las personas pueden enviar mensajes privados a otras personas, o incluso pueden tener mensajes grupales con la gente. Este también tiene su propia aplicación, Facebook Messenger, y se puede acceder desde dentro de la aplicación de Facebook. Facebook tiene un mercado. Aquí es donde la gente puede ir a vender cosas.

Algunas de las vulnerabilidades que Facebook está siendo hackeado. Este es un tema común con todas las aplicaciones de las que hablamos hoy en día. Cuando alguien dice que ha sido hackeado, generalmente eso significa que su contraseña fue comprometida. Alguien descubrió su contraseña o tal vez dejó su teléfono desbloqueado y alguien pudo acceder físicamente a sus aplicaciones de redes sociales. Otra vulnerabilidad se llama catfishing. Catfishing es cuando alguien finge ser alguien o algo que no es. Verás esto donde las personas intentan cometer fraude de una forma u otra fingiendo ser alguien o algo que realmente no son.

Hay muchos tipos diferentes de estafas en Facebook. Verás en alguna parte que alguien te dice que vayas a este enlace y ganes todo este dinero. Eso puede ser peligroso porque ese enlace podría conducir a un virus, o podría conducir a una página en la que alguien solicita información personal. Verá su parte justa de información errónea en Facebook. No todo lo que ves en Facebook es cierto. Asegúrate de hacer su propia investigación.

Hablamos de esto en breve, sobre malware o virus. Si haces clic en un enlace de Facebook, asegúrate siempre de saber adónde te llevará. A veces, podría dirigirte a un sitio web que puede instalar virus y malware en tu computadora. Luego intimidación. El bullying ha sido y sigue siendo rampante en Facebook. Esto afecta severamente a ciertas personas, o las personas se unirán contra otras, o compartirán imágenes o historias sobre otras personas, y eso puede ser muy doloroso. También verás que la intimidación es común en todas estas aplicaciones de redes sociales en su mayor parte. Solo ten eso en cuenta.

Snapchat
Este sitio es famoso por compartir fotos y videos privados y temporales, y por enviar mensajes. Eso significa que si vas a mirar el Snapchat de tus hijos, probablemente no verás nada del contenido que se comparte con ellos o que comparten con otros. Eso puede ser peligroso porque no sabes a qué tipo de contenido está accediendo su joven en Snapchat.

Como se indicó anteriormente, una vulnerabilidad es ser hackeado. Otra vulnerabilidad en Snapchat es compartir la ubicación. Puedes ver dónde están tus amigos en tiempo real en un mapa. Esto es peligroso para las personas que pueden estar acechando a otros. Esto es peligroso porque ha habido robos involucrados. Esto se puede desactivar, pero está activado de forma predeterminada. Solo ten eso en cuenta.

Twitter
Esta es una red social de micro-blogging. Puedes compartir texto o texto multimedia de hasta 142 caracteres. Es un realmente corto diario y el compartir ideas y eventos con otros. Puedes compartir videos, puedes compartir fotos.

Algunas de las vulnerabilidades nuevamente son ser hackeados, intimidación, mucha desinformación, fraude y también podría ser un entorno muy tóxico. Hay mucho menospreciar a otras personas y mucha negatividad en esta aplicación.

TikTok
Se trata principalmente de cortos video diarios y publicación, donde los usuarios pueden transmitir y suscribirse a las transmisiones de los demás. También hay mensajería integrada en la aplicación.

Algunas de las vulnerabilidades son permisos extendidos de aplicaciones. Lo que esto significa es que cuando vayas a instalar TikTok, siempre debes obtener un cuadro que te diga, oye, esta aplicación quiere acceder a estas funciones en su teléfono. Esto podría incluir el GPS de su teléfono que indica dónde te encuentras en el mundo, esto podría incluir el acceso a los contenidos de los otros contactos en tu teléfono, los nombres y números de teléfono. Esto también podría incluir el acceso a los archivos en tu teléfono.

Instagram
Esto incluye compartir fotos y videos. La mensajería también está integrada. Las vulnerabilidades incluyen ser hackeado y estándares de belleza inalcanzables. Es posible que hayas oído hablar de celebridades que retocan sus fotos en Instagram, haciéndolas lucir extremadamente delgadas o haciendo que sus cuerpos se vean de formas inalcanzables. Esto puede hacer que los jóvenes sientan que deberían lucir de esa manera. Es muy peligroso. También hay contenido para adultos en Instagram. Intentan moderarlo, pero todavía hay mucho. Solo ten cuidado con eso.

Discord
Esta es una aplicación de mensajería de voz y texto. También puedes transmitir en vivo tu pantalla o videojuegos. Es popular entre los jugadores. También hay funciones de chat y funciones de chat grupal en Discord. Algunas de las vulnerabilidades son ser hackeados, intimidación, virus. Se trata de virus que pueden incrustarse en Discord a través de algún tipo de medio, como una imagen o un archivo que contiene un código nefasto. El contenido en Discord no está moderado en gran medida, lo que significa que nadie de Discord realmente está monitoreando qué tipo de contenido se publica o escribe en Discord. Esto puede incluir contenido para adultos. También se ha relacionado con la trata de personas. Si su hijo usa Discord, preste atención a para qué lo está usando y si alguien está tratando de hablar con él directamente.

Twitch
Esta plataforma de transmisión de video es popular entre los jugadores. Algunas de las vulnerabilidades son el ser hackeados y contenido para adultos. Puede ser un ambiente muy tóxico. Si alguna vez miras la sala de chat de un transmisor muy popular, verás muchas conversaciones muy negativas, muchas palabras muy inapropiadas.

Reddit
Esta es una plataforma de noticias sociales con foros de discusión. El contenido es calificado por los usuarios. Esto significa que el contenido que los usuarios ven primero es calificado por otros usuarios. Reddit no está moderado en gran medida. Encontrarás una gran cantidad de contenido para adultos, información errónea, intimidación y contenido negativo o inapropiado.

Youtube
Esta es una plataforma para compartir videos. Algunas vulnerabilidades incluyen información errónea y contenido inapropiado. YouTube está moderado pero, desafortunadamente, no pueden prestar atención a todos los videos que se cargan y lo que contienen. El contenido inapropiado o para adultos permanecerá en la plataforma hasta que alguien lo reporta.

Omegle
Aquí es donde puedes chatear por video con extraños. Algunas de las vulnerabilidades que tiene Omegle es que te empareja con un completo extraño en un video así que puedas ver algunas cosas muy inapropiadas que la gente está haciendo, otras personas están diciendo. Ten mucho cuidado con dejar que tus jóvenes usen Omegle . No está moderado, nadie en Omegle supervisa lo que sucede en vivo.

Aplicaciones de mensajería
Casi todas las aplicaciones de redes sociales tienen chat. Las vulnerabilidades incluyen hacking, catfishing, contenido inapropiado y estafas. La mensajería de chat se puede conectar a Wi-Fi para que pueda funcionar sin datos del teléfono celular.

Supervisión de los padres
Los cuidadores tienen la autoridad para monitorear, quitar y/o restringir los dispositivos de sus hijos y/o el acceso a estos dispositivos. Tu trabajador de apoyo comunitario puede ayudarte a pasar por este proceso de establecer restricciones.

Monitorización física de dispositivos. Conoce a qué dispositivos tiene acceso tu hijo: teléfono, tableta, computadora, consola o cualquier cosa que tenga acceso a Internet y pueda tener aplicaciones. Incluso los dispositivos de tu hijo que se envían a casa desde la escuela. Revisa físicamente los mensajes y/o notificaciones en las diferentes aplicaciones de redes sociales. Cada familia tendrá diferentes estrategias en cuanto al control físico.
Conoce el código del teléfono de tu hijo y las contraseñas de las cuentas de redes sociales que usan. No dejes que usen todas las aplicaciones que quieran. Solo permite las aplicaciones que consideres seguras y que el niño tenga la madurez suficiente para acceder.

El monitoreo físico es muy directo y requiere habilidades técnicas mínimas. En cualquier momento, pregunta "Oye, déjame ver tu teléfono". Mira brevemente los mensajes y la actividad. Obviamente, requiere la conformidad del niño, y es posible que no siempre les guste, pero lleguen a algún tipo de acuerdo. "Puedes usar estas aplicaciones si puedo mirar tu teléfono". "Puedes quedarte con este teléfono siempre que yo pueda revisarlo". Establecer expectativas.

Hazle saber a tu hijo que no quieres que hable con extraños o acceda a ciertos tipos de contenido. Hay confianza ahí. Mientras esa confianza no se rompa, continúa permitiéndoles usar el teléfono y las aplicaciones de redes sociales. Hay restricciones basadas en el teléfono. El cuidador puede tener la contraseña del teléfono para monitorear y establecer restricciones para la actividad en línea. Algunos de los ejemplos pueden ser restringir los minutos a los que tiene acceso el joven, prohibir sitios específicos o incluso recibir notificaciones si el joven intenta acceder a sitios restringidos.

Es posible que debas cambiar la contraseña de Wi-Fi o del teléfono. Puede requerir un poco más de conocimiento técnico. Existen aplicaciones de terceros para el control y las restricciones que puedes usar para controlar la actividad en el teléfono, como Net Nanny, Qustodio , Norton Family o FamilyTime .

Apple tiene funciones parentales integradas. Puedes permitirles que descarguen solo aplicaciones específicas que estén calificadas de cierta manera. Puedes monitorear cuánto tiempo pasan en el teléfono, cuánto tiempo pasan en cada aplicación. Es muy poderoso.

Restringir el acceso Wi-Fi
Desconecta físicamente el módem por la noche. Aún mejor, accede a los controles parentales incorporados que no deshabilitarán el Wi-Fi para todos los demás dispositivos de la casa. Se seguirá permitiendo el uso de datos del teléfono celular incluso si su enrutador Wi-Fi está desconectado.

Es importante utilizar contraseñas seguras porque dificulta que los hackers las adivinen. Una contraseña segura suele tener ocho o más caracteres, incluida una letra mayúscula, una letra minúscula, un número y un carácter especial.

Fostering Family

More resources available at
fosteringfamily.com