Primeros Pasos hacia la Seguridad Digital de tus Hijos

Sigue estos consejos y escanea para más información:

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

Controles Parentales:

Pasos Esenciales para Proteger a tus Hijos en Redes Sociales y Dispositivos

TikTok

1. Abre TikTok y haz click en el ícono de Perfil en la parte abajo derecha de la pantalla
2. Oprime "Digital Wellbeing"
3. Oprime "Family Pairing"
4. Selecciona si es una cuenta de "Teen's" o "Parent's"
5. Oprima Continuar y siga las instrucciones para terminar la conexión

TikTok

Instagram

1. Si la cuenta del niño(a) está pública debe cambiar a privada una vez sea mayor de 13 años.
2. Apague el "Geotagging"
3. Bloquee contactos indeseados
4. Evite compartir detalles personales, evite seguir contenido inapropiado
5. Esconda los "Stories" o limite la visibilidad a amigos cercanos "Close Friends"

Instagram

YouTube

1. Asegúrese de tener una cuenta para su hijo(a) de YouTube Kids
2. Acceda entonces a su YouTube con la cuenta parental vinculada
3. Vaya a su foto de perfil y seleccione "Configuración" y luego "Configuración Parental"
4. Selecciona el perfil o la cuenta de tu hijo(a)

YouTube

Facebook

1. Visita el menú de Facebook
2. Oprima " Settings & Privacy" luego "Settings"
3. Revise "Profile" "Account" y "Security" y controle la información que aparece para el niño(a).

Facebook

Apple

1. Toca la opción Activar Tiempo de uso y luego vuelve a tocarla. Selecciona Este es mi [dispositivo] o Este es el [dispositivo] del niño.
2. Toca Restricciones de contenido y privacidad. Si se te pide, introduce el código y activa Restricciones de contenido y privacidad.
3. Impedir contenido explícito y con ciertas clasificaciones. Toca restricciones de contenido y privacidad.

Apple

Android

1. Para poner controles parentales en un dispositivo Android, puedes seguir los siguientes pasos: Abre la aplicación Play Store.
2. En la esquina superior izquierda, toca Menú > Ajustes > Control parental. Configura el control parental y crea un PIN secreto para evitar que otros usuarios cambien la configuración.
3. Toca el tipo de contenido que quieras filtrar.
4. Elige la clasificación de edad que quieras permitir. Toca Guardar.

Android

Microsoft

1. Descarga e instala Microsoft Family Safety en tu PC con Windows.
2. Crea una cuenta de Microsoft Family Safety para ti y para tus hijos.
3. Asigna a tus hijos una cuenta de usuario en el PC con Windows.
4. En Microsoft Family Safety, establece las restricciones y límites que deseas para tus hijos, como el tiempo que pueden estar en línea, los sitios web que pueden visitar y las aplicaciones que pueden utilizar.
5. Configura las alertas y notificaciones que deseas recibir sobre la actividad en línea de tus hijos.

Microsoft

"Las redes sociales no están autorizadas a recopilar información de menores de 13 años, con exepción de que sus padres lo autoricen" Ley COPA, 21 de octubre de 1998.

¿Están Seguros Tus Hijos en Línea?

¡Los 5 Peligros Cibernéticos que Todo Padre Debe Conocer!

Grooming:

Descripción: Adultos malintencionados se hacen pasar por niños para ganarse la confianza de los menores y luego explotarlos de diversas formas, incluyendo el abuso sexual.

Síntomas de la víctima: ·Cambios en el comportamiento · Secretismo · Regalos no explicados · Comunicación con desconocidos · Contenido inapropiado

Prevención: Educar a los niños sobre los peligros de hablar con extraños en línea y fomentar una comunicación abierta para que puedan reportar cualquier comportamiento sospechoso.

Reportar a: ICE- (787) 729-6969, FBI-(787)754-6000

Ciberbullying:

Descripción: Acoso en línea que incluye el envío de mensajes ofensivos, difamación, y la creación de perfiles falsos para dañar la reputación de la víctima.

Síntomas de la víctima: Cambios en el estado de ánimo · Bajo rendimiento académico · Aislamiento· Autolesiones o pensamientos suicidas

Prevención: Fomentar un ambiente seguro para que los niños puedan reportar incidentes de ciberbullying y enseñarles a no participar en comportamientos de acoso.

Reportar a: POLICÍA-(787)793-1234

Sexting:

Descripción: Envío de material sexualmente explícito, como fotos o mensajes, a través de medios digitales.

Síntomas de la víctima: Preocupación excesiva por la privacidad · Contenido explícito · Blackmail · Cambios en el comportamiento · Relaciones inapropiadas

Prevención: Educar a los niños sobre las consecuencias legales y emocionales del sexting, y enseñarles a respetar los límites personales y la privacidad de los demás.

Reportar a: ICE- (787) 729-6969, POLICíA-(787)793-1234

Phishing:

Descripción: Tácticas de engaño para obtener información confidencial, como contraseñas o detalles bancarios, a través de mensajes o correos electrónicos fraudulentos.

Síntomas de la víctima: Compartir información personal · Correos electrónicos sospechosos · Pérdida de acceso a cuentas · Transacciones no autorizadas · Software malicioso

Prevención: Enseñar a los niños a reconocer señales de phishing, como errores gramaticales en los correos electrónicos y URLs sospechosas.

Reportar a: CISA- 1(800) 282-0870, IRS- 1(800)438-4338

Contenido Inapropiado:

Descripción: Acceso a contenido no apto para menores, como pornografía, violencia extrema, o material radical.

Síntomas de la víctima: Exposición a contenido adulto · Lenguaje inapropiado · Imitación de comportamientos violentos · Pesadillas o miedos · Desensibilización

Prevención: Utilizar filtros y controles parentales para restringir el acceso a contenido inapropiado y supervisar el uso de internet de los niños.

Reportar a: POLICÍA-(787)793-1234