Automóviles conectados:
Privacidad y seguridad para las personas sobrevivientes

Los autos más modernos ahora funcionan con sistemas informáticos y de software, y hasta pueden estar conectados a Internet. Sin embargo, esto abre la puerta a que personas malintencionadas puedan abusar o manipular estas nuevas funciones, así como utilizar técnicas antiguas para rastrear o vigilar un vehículo y acechar a alguien. La capacidad de los autos conectados puede permitir que alguien, además del conductor, monitoree la ubicación del auto o controle funciones como el volumen, la velocidad, las alarmas o los seguros de las puertas. Esta funcionalidad puede representar un riesgo significativo para las personas sobrevivientes.

Este recurso ofrece información sobre cómo determinar si su automóvil está siendo monitoreado o controlado de forma remota, además de proporcionar opciones para mejorar su privacidad y seguridad.

Lo que cubre y lo que no cubre

Este recurso se centra en situaciones en las que una persona agresora o acosadora ha tenido acceso físico a su automóvil y/o tiene acceso a una cuenta de automóvil conectado. En particular, analiza las formas en que esa persona podría rastrear su ubicación. Aunque existen otros problemas de privacidad relacionados con los automóviles conectados y los datos que pueden recopilar, este recurso no los aborda.

Hay una gran variedad de autos y la tecnología automotriz evoluciona constantemente. Este recurso es aplicable a muchos tipos de autos, pero puede no ser preciso en todos los casos. Tanto las posibilidades de uso indebido como las formas de recuperar el control pueden variar según la marca, el modelo, el fabricante, el vehículo específico u otros factores.

Los autos conectados utilizan aplicaciones que permiten a los usuarios controlar o supervisar el vehículo, incluso cuando no están físicamente presentes. Este recurso explicará cómo utilizar estas aplicaciones, ofrecerá consejos para aumentar la privacidad y la seguridad, y proporcionará recomendaciones para responder al abuso o acoso.

Automóviles conectados:
Privacidad y seguridad para las personas sobrevivientes

El uso indebido de las funciones de un auto conectado no es la única forma en que alguien puede rastrear un vehículo. Aunque la mayor parte de este recurso se centra en las características de los autos conectados, estas no son las únicas maneras en que le podrían estar rastreando. Antes de abordarlas, enumeramos otras formas en las que podrían rastrear su auto, aplicables tanto a autos conectados como no conectados. Para ir directamente al contenido sobre los autos conectados, haga clic en el enlace que mejor se aplique a su situación:

Si la persona agresora tiene o ha tenido acceso al automóvil .
Si la persona agresora no ha tenido acceso al automóvil .

A continuación, se presentan algunas formas posibles de rastrear un automóvil que no están relacionadas con las funcionalidades de conectividad:

- Los autos más antiguos pueden tener un sistema de navegación incorporado o añadido posteriormente, como OnStar o Garmin.
- Tanto los autos más antiguos como los más nuevos pueden tener dispositivos de diagnóstico a bordo (DAB). Estos dispositivos están diseñados para ayudar a solucionar problemas del vehículo, pero un DAB no autorizado podría ser utilizado indebidamente para rastrear su actividad.
- Existen dispositivos que pueden instalarse y que, ya sea rastrean información para descargarla más tarde, o bien transmiten datos en tiempo real. Estos dispositivos son similares a los que utilizan las aseguradoras en sus programas de descuento por "conductor seguro" o para que los padres monitoreen a los conductores adolescentes.
- Los autos más nuevos y costosos proporcionan a los propietarios registrados información muy detallada que incluye la ubicación, la velocidad, los hábitos de conducción y hasta la posibilidad de controlar algunas funciones a distancia, como el volumen, la velocidad o los seguros de las puertas.
- Las personas agresoras y acosadoras también han escondido otros dispositivos en o sobre los autos. Entre ellos se encuentran los teléfonos básicos o de gama baja (no un teléfono inteligente), los rastreadores GPS y los rastreadores Bluetooth más pequeños. Los rastreadores Bluetooth incluyen:

  - AirTags
  - Etiquetas de rastreo (Tags)
  - Etiquetas inteligentes
  - Rastreadores diseñados para colocarse en los collares de las mascotas, con el fin de recopilar información sobre su ubicación en caso de que se pierdan

  Para obtener más información, lea sobre el Rastreo de ubicación.
- Su teléfono también podría utilizarse para rastrearle sin su conocimiento. Para obtener más información, lea sobre la seguridad y la privacidad del teléfono.
- Las cámaras situadas en lugares públicos, como peajes, fronteras y otros puntos de control, así como las cámaras de vigilancia privadas conectadas a sistemas de datos nacionales (por ejemplo, Flock), también podrían permitir que otra persona descubra dónde ha estado su automóvil.
- Facturas electrónicas de peaje: Si una persona agresora tiene acceso, los estados de cuenta de peaje pueden revelar las rutas, fechas y horas de viaje de una persona sobreviviente.
- Facturas de servicio de vehículos: Si un agresor tiene acceso, las transacciones de servicio pueden revelar lugares y fechas de servicio recientes.
- Estados de cuenta de tarjetas de crédito: Si una persona abusadora tiene acceso a la cuenta, los estados de cuenta pueden revelar las compras cercanas, exponiendo ubicaciones y patrones de viaje.

Antes de empezar, priorizar la seguridad

Utilizar estas opciones puede aumentar su privacidad y seguridad, especialmente si ha compartido automóvil con una persona abusiva en el pasado. Sin embargo, es posible que estas medidas no le protejan de toda vigilancia o monitoreo a distancia. Esto se aplica tanto si la vigilancia se realiza a través de un automóvil como de cualquier otra forma de tecnología.

No hay una forma "correcta" de responder a los abusos y los problemas de seguridad del automóvil. Solo hay formas que se ajustan o no a su situación. Lo que funciona para otra

persona puede no funcionar o no ser seguro para usted. Dé siempre prioridad a la seguridad y confíe en sus instintos. Es posible que la persona abusiva se entere si realiza cambios en la configuración de la cuenta o en las características del automóvil. La persona podría cambiar sus tácticas o intensificar su comportamiento abusivo. En algunas situaciones, hacer cambios también podría borrar pruebas. Estos consejos de seguridad podrían serle útiles:

- Utilice un automóvil "más seguro" o un medio de transporte diferente. Esto se refiere a cualquier vehículo al que la persona agresora no tenga acceso. Considere tomar prestado el automóvil de alguien o utilizar el transporte público para ciertos viajes que desee mantener en privado.
- Obtenga más información. Las funciones de los autos conectados son una de las formas en que una persona abusiva puede vigilar su ubicación o acosarle. Enfrentarse a la violencia, el abuso y el acoso puede ser difícil y peligroso. Las personas defensoras y proveedores de servicios pueden ayudarle a averiguar las opciones y los recursos locales. También pueden ayudarle a crear un plan para su seguridad. Puede comunicarse con una línea de ayuda nacional para que le pongan en contacto con los recursos locales.
    - La información de un fabricante de automóviles individual puede encontrarse en su sitio web. Busque la sección de "privacidad" o "seguridad" en el sitio web.
- Para obtener más consejos sobre el abuso tecnológico y cómo aumentar la privacidad y la seguridad, consulte el conjunto de herramientas de recursos para personas sobrevivientes de Safety Net.

Si la persona agresora tiene o tuvo acceso al automóvil

¿Qué posibilidades hay de que se haga un mal uso?

Si la persona agresora fue alguna vez propietaria legítima del automóvil, es posible que nunca haya desconectado o desincronizado su cuenta de la aplicación del vehículo. Esto podría ser cierto incluso si ahora usted es considerado el propietario único del automóvil o si un tribunal le ha concedido el uso exclusivo del vehículo. En tal caso, la persona agresora

podría seguir teniendo acceso a través de la aplicación, lo que le permitiría saber dónde está el automóvil y controlar ciertas funciones del mismo.

Algunas compañías permiten a los propietarios añadir conductores autorizados. Si usted es el único propietario, considere si alguna vez añadió a alguien más como conductor autorizado o si la persona abusiva pudo haber utilizado su cuenta para añadirse a sí misma. Si a una persona nunca se le dio de baja como conductor autorizado, aún podría utilizar las funciones del automóvil.

También existe un sistema llamado Android Automotive OS (AAOS) que viene incorporado en algunos automóviles. Proporciona infoentretenimiento, navegación, mensajería y control de algunas funciones del vehículo. No se utiliza en un teléfono, sino desde el interior del automóvil, y permite descargar aplicaciones, igual que en un teléfono o una tableta. Wikipedia tiene una lista de modelos de automóviles que disponen de AAOS. Apple actualmente está desarrollando un sistema equivalente a AAOS.

El AAOS es especialmente preocupante si una persona agresora o acosador puede tener acceso físico a su automóvil. Esto se debe a que el AAOS almacena sus aplicaciones y datos en el propio vehículo. Una persona agresora que pueda entrar en el automóvil podría acceder al AAOS y ver cómo lo ha utilizado, incluyendo mensajes enviados a través del sistema o las rutas por donde ha conducido el vehículo.

¿Cómo puedo recuperar el control?
Si cree que la persona agresora conoce las contraseñas de su cuenta de automóvil, puede cambiarlas (si se siente seguro(a) haciéndolo). Además, es posible que tenga otras opciones para añadir seguridad a estas cuentas, dependiendo de la aplicación.

Disponemos de un recurso que analiza diversas opciones para mejorar la seguridad de sus contraseñas. Explica las razones por las que las personas usan contraseñas débiles o las reutilizan. También ofrece consejos para tener una protección sólida sin complicaciones. Además, puede consultar nuestro recurso de Seguridad de dispositivos y cuentas, donde se

examinan las opciones de seguridad tecnológica de manera más general. La mejor opción para usted dependerá de su situación. Ambos recursos le ayudarán a encontrar lo que mejor se adapta a sus necesidades.

A veces, puede obtener ayuda hablando directamente con la compañía automovilística. Otra opción es que un abogado hable con la compañía en su nombre. Las empresas suelen tener información de contacto en sus sitios web. Las solicitudes de atención al cliente son atendidas inicialmente por personas con poco poder dentro de la empresa, por lo que podría necesitar insistir para escalar la cuestión (enviarla a alguien con mayor rango). Es posible que tenga que hacerlo más de una vez.

Si la persona agresora no ha tenido acceso al automóvil

¿Qué posibilidades hay de que se haga un mal uso?
En algunos casos, una persona agresora puede conocer o adivinar la contraseña de su cuenta de la aplicación del automóvil. En ese caso, podría acceder a su cuenta y utilizar sus funciones para controlar el vehículo. Si los datos de uso del automóvil están almacenados en la cuenta, podría conocer sus actividades de esa forma.

Si cree que su vehículo está siendo rastreado, pero la persona nunca ha tenido acceso a la cuenta que usted conozca, considere otras formas en que la persona agresora podría estar vigilando el automóvil. También, considere hablar con una persona defensora. Sin acceso ni al vehículo ni a la cuenta, es menos probable que la persona agresora esté utilizando la conectividad del automóvil. Podría estar utilizando un rastreador colocado en el automóvil, un teléfono escondido en el vehículo u otros medios.

¿Cómo puedo recuperar el control?
Si la persona no ha tenido acceso físico al automóvil, pero cree que aún le controla o vigila, el problema podría ser que conozca la contraseña de su cuenta. Desde un dispositivo seguro, cambie la contraseña. En la sección "¿Cómo puedo recuperar el control?"

encontrará más información sobre la seguridad de las contraseñas y la autenticación multifactor.

La compañía que proporciona el servicio inalámbrico para su automóvil almacena datos sobre cómo utiliza usted su servicio. Si la persona agresora conoce la contraseña de su cuenta con esa compañía, podría acceder a esta información. Esto también podría suceder si estuviera en un plan familiar con usted. La sección "Otras cuestiones relacionadas: Planes familiares y aplicaciones de las operadoras de telefonía celular" explica cómo recuperar el control en este caso.

¿Cómo puedo documentar el uso indebido de mi vehículo?

Si ocurre algo que alguien pueda ver u oír mientras está en el automóvil, es posible documentarlo con una cámara. Aquí hay algunos ejemplos de ello:

- El sonido de las puertas del automóvil cerrándose con llave cuando usted no las ha cerrado.
- Una imagen del automóvil cuando no responde cuando intenta recuperar el control. Por ejemplo, podría ser un video en el que intenta desbloquear las puertas del automóvil y estas no se abren.
- La presencia del automóvil del agresor en su destino, lo que indica que le siguen o vigilan.

Si utiliza una cámara para documentar el uso indebido de su automóvil, es mejor que sea en un dispositivo al que el agresor no tenga acceso. También conviene evitar conectarla al automóvil para que el agresor no pueda acceder a ella. Todos estos servicios requieren algún tipo de cuenta. Los datos de la cuenta pueden contener pruebas del acceso o la actividad de la persona agresora. Por ejemplo, podrían mostrar que alguien entró en su cuenta desde la ciudad donde vive el agresor.

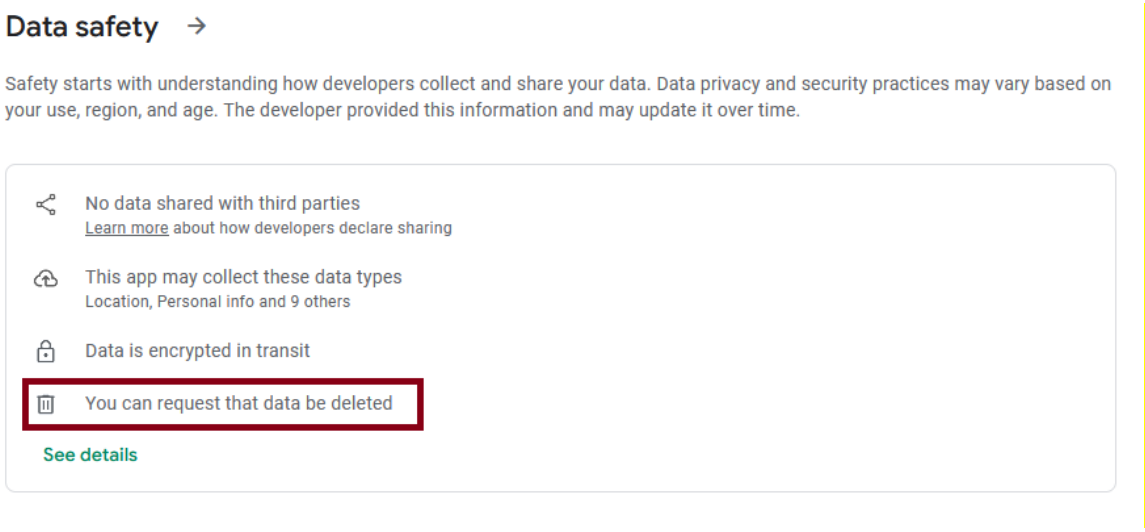
Puede obtener más información sobre cómo documentar los abusos facilitados por la tecnología (no solo los relacionados con los automóviles) en estos recursos:

- Consejos de documentación para personas sobrevivientes (Safety Net).

- Cómo reunir pruebas de abuso tecnológico para el tribunal (Safety Net y NCJFCJ).
- Cuestiones relativas a las pruebas en casos relacionados con la tecnología (WomensLaw.org).
- Registro de documentación de incidentes y conductas de acoso (SPARC).

Preocupaciones y consejos sobre la privacidad de los datos

Algunas empresas tecnológicas permiten a los usuarios borrar algunos o todos los datos que han almacenado sobre ellos, dependiendo de su lugar de residencia. Para ver qué derechos de privacidad tiene por ley, busque su estado en la parte "verde" de este gráfico. Si se encuentra en esta parte de la tabla y hay una "X" bajo "Derecho a eliminar", entonces las empresas deben permitirle eliminar sus datos. Las empresas pueden seguir permitiéndole borrar datos si vive en otro estado, aunque no estén obligadas a hacerlo. Para muchas aplicaciones, puede verificar si permiten borrar datos a todos los usuarios en sus páginas de Google Play Store. Desplácese hasta la sección Seguridad de los datos. Si dice "Puede solicitar que se borren los datos", entonces puede borrar los datos independientemente del estado en el que viva.



La *forma* de borrar los datos será diferente para cada aplicación o cuenta. Pruebe a utilizar Google u otro motor de búsqueda para buscar "eliminar datos" seguido del nombre de la aplicación o empresa, para encontrar instrucciones específicas.

Otros temas relacionados: Planes familiares y aplicaciones del operador

En un automóvil conectado, una empresa de telecomunicaciones puede proporcionar la conectividad inalámbrica. Estas empresas se conocen como "operadoras de telefonía celular"o *"carriers",* como Verizon y AT&T. También pueden ofrecer aplicaciones relacionadas con el automóvil a quienes ya utilizan sus servicios telefónicos. Esta conectividad puede proporcionarse a través de funciones integradas en el vehículo, activadas mediante una prueba gratuita o una suscripción de pago, o a través de un dispositivo independiente que se conecta al puerto de diagnóstico a bordo (DAB) del automóvil. Las aplicaciones del operador pueden proporcionar servicios Wi-Fi al vehículo, seguimiento de la ubicación, servicios de detección de colisiones y otras funciones.

¿Qué posibilidades hay de que se haga un mal uso?

Muchas personas utilizan planes familiares para el servicio celular y de datos. Si una persona agresora es parte de un plan familiar con usted, podría acceder a la cuenta y ver cómo ha utilizado los servicios. Esto podría incluir el uso de los servicios del automóvil o los lugares a donde ha viajado. También podría ser un problema si la persona agresora conoce o puede adivinar la contraseña de su cuenta con una compañía telefónica.

¿Cómo puedo recuperar el control?

La Ley de Conexiones Seguras de 2022 facilita a las personas sobrevivientes el abandono de los planes familiares. Gracias a esta ley, puede dejar un plan familiar aunque no sea el titular principal del plan. Puede hacerlo de forma ágil y sin tasas de rescisión. Dependiendo de su estado, es posible que tenga que aportar documentación. Cada compañía tiene sus propios procesos (T-Mobile, Verizon, AT&T).

Al igual que otras cuentas, su cuenta telefónica puede tener una contraseña. Si usted es la persona propietaria de su plan telefónico y cree que una persona agresora conoce su contraseña, puede cambiarla para asegurarse de que no pueda acceder a ella. También es posible añadir otras funciones de seguridad a su cuenta con su compañía telefónica. Consulte la sección "¿Cómo puedo recuperar el control?" para obtener enlaces a nuestros recursos sobre seguridad de contraseñas y cuentas.

©2025 Red Nacional para Acabar con la Violencia Doméstica, Proyecto Red de Seguridad.
Apoyado por US DOJ-OVW Grant# 15JOVW-23-GK-05170-MUMU. Las opiniones, resultados y conclusiones o recomendaciones expresadas son de los autores y no representan necesariamente los puntos de vista del Departamento de Justicia de los Estados Unidos.