Pequeño Negocio, Gran Amenaza

Mejores Prácticas para Vehículos Conectados en línea

Antecedentes e Introducción

El propósito del siguiente documento es para ayudar a su negocio a tomar las medidas necesarias para utilizar las mejores prácticas de seguridad, si usted tiene un vehículo conectado al Internet o si tiene dispositivos para servicios como Wi-Fi en el vehículo, OnStar, altavoces inalámbricos, etc…

Este documento discute las prácticas de seguridad más básicas que **TODOS** deberían seguir como punto de partida. Si usted siente que pertenece a una categoría más compleja, es altamente recomendable que contacte a su proveedor de IT para futura dirección y asistencia.

Esta no es una lista comprensiva de todos los posibles procedimientos de seguridad, como muchas de las necesidades más avanzadas de IT dependen de la naturaleza del negocio y si el negocio tiene que cumplir con requerimientos de conformidad con su industria

- **Sea proactivo con sus precauciones de seguridad** para asegurar que potencialmente no sea víctima de un ataque de seguridad; siempre actualice sus sistemas de software como ha sido instruido por su fabricante de automóviles (de igual manera como hace con su teléfono celular, tableta o laptop) para asegurar que tiene los últimos sistemas de seguridad en su vehículo.

- **Visite distribuidores autorizados y tiendas de reparación**; haga preguntas e investigue acerca del entrenamiento y certificaciones con relación al trabajo con tecnologías de vehículos conectados. Este no es un trabajo para el mecánico con conocimientos básicos, ya que estos sistemas usan tecnología altamente compleja.

- **Infórmese acerca de las tecnologías usadas en su vehículo**, y asegúrese de encontrar los recursos para mantenerse informado de potenciales brechas de seguridad. Si su fabricante del vehículo o proveedor dispone de una hoja de noticias suscríbase; monitoree las noticias y preste atención particular a las historias relacionadas con vehículos conectados y luego determine si las noticias descritas son aplicables a usted. Conozca con anticipación a quien tiene que llamar: su proveedor, fabricante, tienda de reparaciones, para consultar en este tipo de cuestiones.

- **Proteja su información personal, información del vehículo y contraseñas** de que caigan en las manos equivocadas. Con tan solo mínima información un hacker determinado puede tener acceso a su vehículo, y a través del vehículo a todo lo que está conectado a este.

Desarrollado por el SBDC de Michigan con apoyo de la Administración de Pequeños Negocios de los U.S. y la Corporación de Desarrollo Económico de Michigan.

Pequeño Negocio, Gran Amenaza

- **Use tan solo dispositivos que han sido probados y verificados en el mercado**; verifique con el fabricante del vehículo, para asegurarse que el uso de los dispositivos han sido aprobados y que estos dispositivos son compatibles con la tecnología en el vehículo para que evite brechas de seguridad.