MERCURY INSURANCE

HACKABLE CARS: GLOSSARY OF RELEVANT TERMS

Autonomous Vehicles

Autonomous vehicles are self-driving vehicles equipped with technology to navigate roadways without intervention from a human driver. These vehicles are equipped with an advanced Laser Illuminating Detection and Ranging (LIDAR) system, which creates a 3D map by bouncing a laser beam off of surfaces to create a computer view of the surrounding environment. These vehicles also use GPS maps, radar, sonar, cameras and an array of sensors to avoid real-world collisions and hazards.

Connected Car

A connected car is a vehicle that has internet access through an installed mobile hotspot or in-car Wi-Fi. Vehicles with built-in Bluetooth compatibility, GPS navigation systems and newer infotainment systems use outside networks and are connected to the internet.

Control Area Network (CAN)

Commonly shortened to "CAN," this system is made up of a series of lines that allow data transfer and communication between various computer systems within a vehicle. The CAN regulates a vehicle's command network.

Cybersecurity

Cybersecurity is any measure or means taken to protect and secure electronic data from unauthorized or criminal use.

Electronic Control Units (ECU)

Commonly referred to as a vehicle's "ECU," this controls the electrical system and its subsystems. The ECU monitors engine operation (i.e., airflow, idle speed, ignition timing, and other important vehicle operations).

Engine Disabler

An engine disabler is a device automobile owners can connect to their vehicle to stop the engine from starting.

Hacker

Hacker is a term used in reference to an individual who uses a computer to access another party's computer and the files on it. While companies can hire hackers in a research capacity to test the overall security of their products, those who hack into data without authorization are considered cybercriminals.

MERCURY INSURANCE

In-car Wi-Fi
A wireless network that is built into the vehicle. Today, this is considered a luxury feature. Manufacturers have begun including built-in Wi-Fi routers in factory installed components. These components are compatible with an array of devices and are usually under warranty.

Infotainment System
Also known as in-vehicle entertainment (IVE) or in-car entertainment (ICE), infotainment systems provide in-car audio and/or video entertainment. This connected hardware has become increasingly popular in modern vehicles, providing access to satellite radio and apps and can provide access to hands-free voice and audio controls from the steering wheel or dashboard.

Key Fob
A key fob is used in modern vehicles with keyless entry. The small device generates random codes and is used to wirelessly unlock a vehicle. Key fob codes are hackable, and transmissions between the device and vehicle can be intercepted to gain physical entry.

Mobile Hotspot
A personal device that can create a Wi-Fi connection that allows devices within its range to connect to the internet. They are portable and serve as a link between Wi-Fi capable devices (i.e., phones, tablets and laptops) and cellular networks.

On-Board Diagnostics-II (OBD-II)
Modern vehicles are equipped with On-board diagnostic ports so that mechanics can easily access computer information and read error codes. The OBD-II is a second generation, standardized diagnostic port, and it's included on most vehicles purchased after 1996. While the location of the OBD-II port differs from vehicle to vehicle, the port is typically located on the inside of the car underneath the dashboard.

Smartphones
Smartphones are cellular phones that perform many of the functions of a computer, with internet access and GPS capabilities as well as an operating system capable of running downloadable applications. They can be synced to vehicle functions via Bluetooth making them vulnerable to being hacked and used to unlock and start a vehicle remotely. The vehicle's location can also be tracked via GPS using a smartphone.

Vehicle Cybersecurity
Vehicle cybersecurity refers to any measure or means taken to secure a vehicle's connected systems from any unauthorized or criminal entry or use.

Vehicle Hacking
Vehicle hacking refers to any unauthorized or criminal access to a vehicle's connected systems whether to access personal information, gain entry to a vehicle or take control of vehicle functions.