Hacking a Car

https://auth0.com/blog/car-hacking-and-cybersecurity-in-automotive-industry/

Car hacks are real, and they're happening right now. Hackers are remote controlling cars, and they're doing it more often. Manufacturers aren't protecting drivers' information or security. There are too many hackers out there who want to steal people's personal information.Cars need to be connected to the internet to work properly. Hackers could cause problems by sending messages to the brakes and locking drivers inside cars. Manufacturers should improve their cybersecurity programs to protect vehicles from hackers.Automotive cyber security has become an increasingly important issue over the past few years. Manufacturers must do more to protect their cars from hackers. Here are some examples of how this happens.

-"Hackers can use tire pressure monitoring systems to cause problems with your vehicle’s tires.

-"They can also hack your car’s electronic control unit to turn on the air conditioning without your permission, or to start the engine without your consent."The article mentions how hackers can hack into the onboard computer, and disable the brakes and engine. This could be done by hacking into a car's ECU (Electronic Control Unit).MP3 malware is a type of malicious software that can infect a computer's audio player, such as an iPhone or iPod Touch.

Hackers can use this technology to take control of vehicles remotely.Power Locks:

- Some cars have power locks, which lock the car's doors when the vehicle is turned off.

Extended Key Fob Range:

- A thief can use a wireless key fob to unlock your car door when you're up to 30 feet away from the vehicle.-" Driving data downloads": Your car records how fast you go, how long you spend in traffic jams, etc., and sends this data to your insurance provider. This allows them to determine how much money you should pay each month.

-"Smartphone access": Hackers may be less likely to target your car's systems and more interested in hacking your smartphone.1. Air conditioner systems are vulnerable to hackers.

2. Hackers can release hot air in the summer.

3. Hackers can turn on the passenger side seat warmer.

4. Hackers can disable windshield wipers.

5. Hackers can spray windshield cleaning fluid onto the windshield.

Automotive mobile apps are great for consumers, but they can also be used by hackers to access your vehicle. Hackers can use weak passwords or exploit vulnerabilities in apps to gain access to your vehicle. You should never download an app without verifying its authenticity. You should also change any default passwords you may have set up for your vehicle.Manufacturers should make sure that their products are secure by using security features such as encryption, authentication, and access control. They should also be aware of the latest threats and vulnerabilities and use them to improve their products' security. Finally, they should ensure that they get proper training and certification before selling their products to customers.

There is no one-size fits all solution for car cybersecurity. Manufacturers should focus on securing the most vulnerable parts first.