The FBI Warns That Car Hacking Is a Real Risk

March 17, 2016 By: Andy Greenberg Wired

http://www.wired.com/2016/03/fbi-warns-car-hacking-real-risk/

IT'S BEEN EIGHT months since a pair of security researchers proved beyond any doubt that car hacking is more than an action movie plot device when they remotely killed the transmission of a 2014 Jeep Cherokee as I drove it down a St. Louis highway. Now the FBI has caught up with that news, and it's warning Americans to take the risk of vehicular cyber sabotage seriously.

In a public service announcement issued together with the Department of Transportation and the National Highway Traffic and Safety Administration, the FBI on Thursday released a warning to drivers about the threat of over-the-internet attacks on cars and trucks. The announcement doesn't reveal any sign that the agencies have learned about incidents of car hacking that weren't already public. But it cites all of last year's car hacking research to offer a list of tips about how to keep vehicles secure from hackers and recommendations about what to do if you believe your car has been hacked—including a request to notify the FBI.

"Modern motor vehicles often include new connected vehicle technologies that aim to provide benefits such as added safety features, improved fuel economy, and greater overall convenience," the PSA reads. "Aftermarket devices are also providing consumers with new features to monitor the status of their vehicles. However, with this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cyber security threats."

The FBI and DOT's advice includes keeping automotive software up to date and staying aware of any possible recalls that require manual security patches to your car's code, as well as avoiding any unauthorized changes to a vehicle's software and being careful about plugging insecure gadgets into the car's network. Most of those tips stem directly from last year's research demonstrations: After hackers Charlie Miller and Chris Valasek hacked the Jeep in July, Chrysler issued a 1.4 million vehicle recall and mailed USB drives with software updates to affected drivers. And the next month, researchers from the University of California at San Diego

showed that a common insurance dongle plugged into a Corvette's dashboard could be hacked to turn on the car's windshield wipers or disable its brakes.

The announcement also notes that drivers should be careful about offering physical access to their vehicles to strangers. "In much the same way as you would not leave your personal computer or smartphone unlocked, in an unsecure location, or with someone you don't trust, it is important that you maintain awareness of those who may have access to your vehicle," the announcement reads. (If only the FBI felt quite so strongly about keeping intruders out of your iPhone.)

Not much in the FBI's warning is new information, says Chris Valasek, one of the two Jeep-hacking researchers. But he says the imprimatur of the FBI could make the threat of car hacking real for anyone who hasn't considered the growing risk of digital attacks on connected vehicles. "It seems super delayed," says Valasek. "But it's good advice…people take the FBI seriously."

Valasek says the most significant part of the announcement may be its request that anyone who suspects their car has been hacked to get in contact with the FBI, along with the car manufacturer and the National Highway and Traffic Safety Administration. Until now, Valasek says, he and his fellow Jeep hacker Charlie Miller have themselves been bombarded with messages—credible and not-so-credible—from people who believe they're car hacking victims. "Charlie and I get emails all the time from people who say 'my car's been hacked!'" he says. "The FBI is more than welcome to take that over."