MERCURY INSURANCE

HACKABLE CARS FAQ

Reports of vehicle hacking have been in the news more often during the past year. Mercury Insurance worked with car hacking expert, Craig Smith, to provide the following list of frequently ask questions to help consumers learn how to protect themselves and their cars from a potential cyberattack.

Q: How do I know if my vehicle is at risk of being hacked?

A: There are many factors that go into determining a vehicle's risk. If you're specifically concerned about remote hackers, as opposed to those who have physical access to the car, look at the wireless systems your vehicle supports. For example, does the vehicle have telematics, satellite or digital radio, internet, Bluetooth or wireless key fobs?

Wireless systems can provide entry points for an attacker over varied distances. This is also true for aftermarket components that are added to vehicles such as dongles plugged into the car's OBD-II port to monitor performance or for insurance reasons.

Q: Are some vehicles (years, makes or models) more hackable than others? Can older vehicles be hacked?

A: Newer vehicles have what we call a higher "attack surface." This means there are more areas for a hacker to target to look for vulnerabilities. Older vehicles with less technology are generally less susceptible to attacks, but adding aftermarket technology, like a dongle some insurance companies use to monitor driving habits, can increase the risk. Mercury doesn't use this technology, which is good news for our customers.

It should also be noted that while newer vehicles tend to have a larger attack surface, they also have more safety features that can help minimize or avoid injury in a collision, so you should consider that as well.

Q: How can I protect my vehicle from being hacked?

A: Disable wireless services that you aren't using. If your auto manufacturer provides information on your vehicle's wireless features, decide which ones are the most important and only enable those options. If you wish to use a dongle in your vehicle, try to use it sparingly and take it with you when you leave the car.

Q: What are the common signs I should look for to see if my vehicle has been hacked?

A: Hacked vehicles are still a very rare thing to find in public. There really aren't any telltale signs a vehicle has been hacked. If your vehicle is performing strangely, take it to your dealer to discuss the problem. It could be a normal configuration problem or a bug in the particular software version the car's computer is using.

MERCURY INSURANCE

Q: If I think my vehicle has been hacked, what should I do?

A: Take it to your dealer to discuss the problem. Keep in mind it is currently very unlikely that the vehicle was hacked. However, it is always good to be vigilant and there could be something else wrong with the vehicle.

Q: What is the difference between a regular vehicle malfunction and a malfunction that's the result of a hack? Is there a way to determine which one occurred?

A: A regular vehicle malfunction often occurs when a physical device fails. However, with software-based systems, it can also be a bug in the software. Hacked devices do not fail but instead, are used in ways that were unintended by the manufacturer. The fact that devices do not completely fail make them harder to detect and determine the difference between a software bug and an intentional hack. There currently are no ways to determine if your vehicle has been hacked other than bring it to the dealer.

Q: How do hackers take control of a vehicle?

A: Remote hackers will look for vulnerabilities in a device that is capable of wireless communications such as Wi-Fi, cellular or radio waves. Once an attacker has access to a vehicle, they could target the data held by the vehicle or other parts of the vehicle system.

Q: In the event that a vehicle is hacked while on the road, what steps should I take to regain control of the vehicle?

A: The thought of a hacker remotely driving your vehicle is scary. If you find yourself in a situation where you don't seem to have control of the vehicle then stop and power it off right away. Have the vehicle towed to a shop for inspection.

Q: How do hackers gain access to a vehicle to steal its contents or the vehicle itself and what can I do to protect against these actions?

A: Most vehicle break-ins are still physical; however, we are seeing some attacks using electronic key fobs. These attacks often trick the vehicle into thinking the owner's keys are closer than they really are, which unlocks the vehicle but, usually, does not allow the criminal to steal the car, just the contents. Some cars are stolen after a break-in by using a key programmer and programming a blank key to work with the intended vehicle.

Consumers who have wireless key entry systems – which allow one to open car doors without pressing a button or inserting the key into the lock – can take additional precautions by putting their keys in a metal drawer at night.

Q: Is there a way to determine whether vehicle hacking was the cause of a collision?

A: Potentially. It varies on the vehicle, the data collection that was taking place, and the type of hack and collision that occurred. Just like a black box for a plane cannot always determine the cause of an accident, a vehicle's disaster recovery system may not be able to either.

Q: If my vehicle is deemed at-risk for hacking, what preventative steps can I take to avoid or minimize the risk?

A: Disable the components that have the most risk. For instance, if the radio unit is the culprit you can disable it or replace it.