Mercury Insurance and Auto Security Expert Craig Smith Talk in October 2016 to Inform Consumers About Preventing Vehicle Cyberattacks

The 'Car Hacker's Handbook' author shares his knowledge of vehicle cybersecurity to help protect the public.

Los Angeles, Calif. (PRWEB) November 15, 2016 -- Connected vehicle technologies allow today's consumers to benefit from improved safety equipment and the convenience of home. While great selling points for car shoppers, this elevated level of connectivity also makes vehicles more vulnerable to cyberattacks.

Mercury Insurance (NYSE: MCY), with help from Craig Smith, the author of "The Car Hacker's Handbook" and founder of Open Garages, a community for sharing and collaborating on automotive research, is alerting consumers about how their cars might fall victim to vehicle hacking and what they can do to protect against it.

"Our focus at Mercury is to keep roads safe for drivers and pedestrians, and the threat of vehicle cyberattacks should be a real concern for everyone who drives," said Tom Coyne, auto line lead for Mercury Insurance. "Craig's expertise is helping us inform consumers to be aware that, while their vehicles are safer now than ever before, they might also be more of a target for thieves or ill-intentioned hackers."

Smith has worked in the security industry for more than 20 years and with the auto industry for five. He shares his insights in this Q&A.

Question: How can consumers determine if their vehicles are at risk of being hacked?

Craig Smith: There are many factors that go into determining a vehicle's risk. If consumers are specifically concerned about remote hackers, as opposed to those who have physical access to the car, then they should look at the wireless systems the 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.

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

Smith: Newer vehicles have what we call a higher 'attack surface.' This means there are more entry points hackers can exploit. Older vehicles with less technology are generally less susceptible to cyberattacks, but adding aftermarket technology, like a dongle used by some insurance companies to monitor driving habits, can increase the risk.

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.

Question: How can consumers protect their vehicles from being hacked?

Smith: Disable wireless services they are not using. If their auto manufacturer provides information on their vehicle's wireless features, they should decide which ones are important to them and only enable those options. If they wish to use a dongle in their vehicles, they should try to use it sparingly and take it with them when they leave the car.

Question: What are the common signs consumers should look for to see if their vehicles have been hacked?

Smith: 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 someone feels their vehicle is performing strangely, they should take it into their 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.

Question: What should a consumer do if they believe their vehicle has been hacked?

Smith: Take it into their 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.

Question: 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?

Smith: 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 for a consumer to determine if their vehicle has been hacked other than bring it to the dealer.

Question: How do hackers take control of a vehicle?

Smith: 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, the attacker could target the data held by the vehicle or other parts of the vehicle system.

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

Smith: The thought of a hacker remotely driving your vehicle is scary. If consumers find themselves in a situation where they do not seem to have control of the vehicle, they should stop and power it off right away. Then they should have the vehicle towed to a dealer for inspection.

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

Smith: Most vehicle break-ins are still physical; however, we are seeing some attacks using electronic key fobs. These attacks 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. This is mainly a concern for people who park on the street, live near the street or whose job is near their car. This type of attack involves

amplifying the key fob's signature.

Some cars are stolen after a break-in by using a key programmer to program a blank key.

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 or refrigerator at night. The goal is to block out or reduce the signal of the keys so that they are not transmitting when not in use.
Question: Is there a way to determine whether vehicle hacking was the cause of a collision?

Smith: Potentially. It varies by 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.

Question: If a vehicle is deemed at-risk for hacking, what preventative steps can a consumer take to avoid or minimize the risk?

Smith: They can disable the components that have the most risk. For instance, if the radio unit is the culprit they can disable it or replace it.

"We continuously review the automotive marketplace, so we can provide consumers with important information about how to protect themselves, families and property, whether it's about the dangers of distracted driving, teen driving safety or, now, vehicle hacking," adds Coyne. "And Mercury doesn't use dongle technology because we don't want to increase our customers' risk of a cyberattack, which we think they appreciate."

Mercury Insurance has an infographic that helps consumers answer the question "How Hackable is Your Car?" Visit https://blog.mercuryinsurance.com/how-hackable-is-your-car/ to see how your car scores.

Click here for a Glossary of Terms to define the hackable vehicle features outlined above.

ABOUT MERCURY INSURANCE
Mercury Insurance (MCY) is a multiple-line insurance organization predominantly offering personal automobile, homeowners and commercial insurance through a network of independent agents in Arizona, California, Florida, Georgia, Illinois, Nevada, New Jersey, New York, Oklahoma, Texas and Virginia. Since 1962, Mercury has specialized in offering quality insurance at affordable prices. For more information visit www.mercuryinsurance.com or Facebook and follow the company on Twitter.

###

Contact Information
Wendi Sheridan
Pacific Communications Group
(424) 903-3644

Online Web 2.0 Version
You can read the online version of this press release here.