

Worrying aspects about security (and lack of it) with modern cars...

Published: October 24, 2018

Author:

Online version: <https://www.wheels-alive.co.uk/worrying-aspects-about-security-and-lack-of-it-with-modern-cars/>



Half of drivers with keyless technology are concerned about car hacking...

Worrying figures...

16 per cent of drivers or someone they know have experienced car hacking.

99 per cent of drivers are unaware of all the major digital hacking threats their car might face.

79 per cent of people don't know if their car insurance would cover hacking.

Despite 110 car models being vulnerable to one of the most prevalent digital attacks – theft of the vehicle via hacking of the keyless entry and ignition system (Reference 1) – only 50 per cent of drivers with keyless access are concerned about their car being stolen, a new study shows (2).

Research from the UK's price comparison website MoneySuperMarket highlights the



security flaws that hackers can exploit to attack your vehicle, from key jamming to phone phishing for car access. The results reveal not only the hacking methods to which your car may be vulnerable, but also the nation's level of understanding of the overall problem.

Figures from the Office of National Statistics (ONS) show that there may be a resurgence of vehicle crimes after a long period of decline, with an overall 19 per cent increase in vehicle crime and a 29 per cent increase in crimes related to vehicle interference since 2014 (3). The increasing prevalence of car technology creating opportunities for hackers is thought to be a contributing factor, making the deployment of up-to-date security measures more important than ever.

Hacking methods

One of the most common approaches used by hackers is to attack cars with keyless access. Criminals use a relay system to access the vehicle by amplifying a key signal from inside a property so that it reaches the car on the driveway.

19 per cent of drivers already disable their keys when not in use, by either placing them into a secure holder such as a microwave or a Faraday cage to block the signal (2).

Additional security weak spots include:

Phone phishing for car access - Most people are aware of phishing scams in general, but what's less widely known is that hackers can email you malicious links that then connect to a car's WiFi features, if it has them, and take control (4).

Local remote control apps - There are a number of car tracking apps on the market that allows users to locate, start and control their cars from their phones. While these can be handy for those with Internet connected cars, they also open the users up to hackers who have proved they can manipulate the system to locate, unlock and even cut out the engine of nearby cars on the system remotely (5).

Tyre pressure monitor systems - Using low-cost, readily available equipment, hackers can



use sensors inside a vehicle's tyres to display false tyre pressure readings – and more worryingly, track the car (6).



Driver concerns

Despite the risks, 13 per cent of drivers are still excited about cars with automation, Wi-Fi hotspots and biometric access. However, 22 per cent are more wary and consider this new technology to be a security threat.

It seems too that those who were concerned may be right to be worried – 16 per cent of drivers or someone they know have experienced a form of car hacking. Additionally, there is a lack of knowledge surrounding the cover available for victims of these attacks, with 79 per cent of people admitting they don't know whether their car insurance policy would cover them if their vehicle were hacked.

Tom Flack, Editor-in-Chief at MoneySuperMarket, commented: "Car hacking is little



understood but a very real threat. Manufacturers are adding increasing amounts of technology to our vehicles, and new technology comes with new risks that drivers need to understand and guard against.

We recommend fully researching a vehicle and its capabilities and limitations before purchase, and getting to know a vehicle you already own to make sure you're aware of any potential security flaws. Sometimes an old fashioned security method, such as a steering lock, can be all that's needed to protect against criminals.

As far as hacking activity such as keyless theft - so-called 'relaying' - is concerned, insurers will pay out providing the owner/driver has taken reasonable care to protect their property. Owners of cars deemed by insurers to be a particular risk of keyless theft may find they are charged higher premiums as a result."

To find out how you can protect against the major security flaws in vehicles on the road today, and to find out more about how British drivers are responding to the issues, see the full study on the MoneySuperMarket website [here](#).

References

1. <https://www.express.co.uk/life-style/cars/806889/Keyless-entry-car-keys-hack-theft-warning>
2. MoneySuperMarket survey data conducted across 1000 UK car owners 02/08/2018 - 08/08/2018 in association with OnePoll.
3. <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables>
4. <https://interestingengineering.com/what-is-car-hacking-what-can-you-do-prevent>
5. <https://www.zdnet.com/article/flaw-connected-alarm-system-exposed-vehicles-remote-hackin>



g/ 6 https://www.schneier.com/blog/archives/2016/09/hacking_wireles.html

