CarGurus®

Data Security in Connected Cars

Facilitating everything from voice-activated texting to your favorite virtual assistant, connectivity has finally made its way to personal vehicles. Along with all the perks it's introduced come some notable risks. In a two-part study, we first asked drivers about their connectivity habits. Then, we quizzed them on said risks. The results? Jaw dropping.
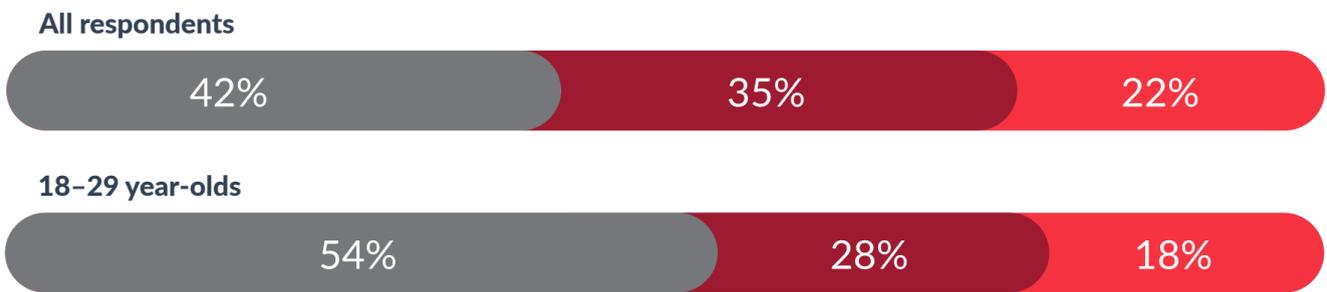
Connected & Carefree

Most drivers connect their smartphones to their cars, yet only 22% find connected cars to be a serious data security threat.
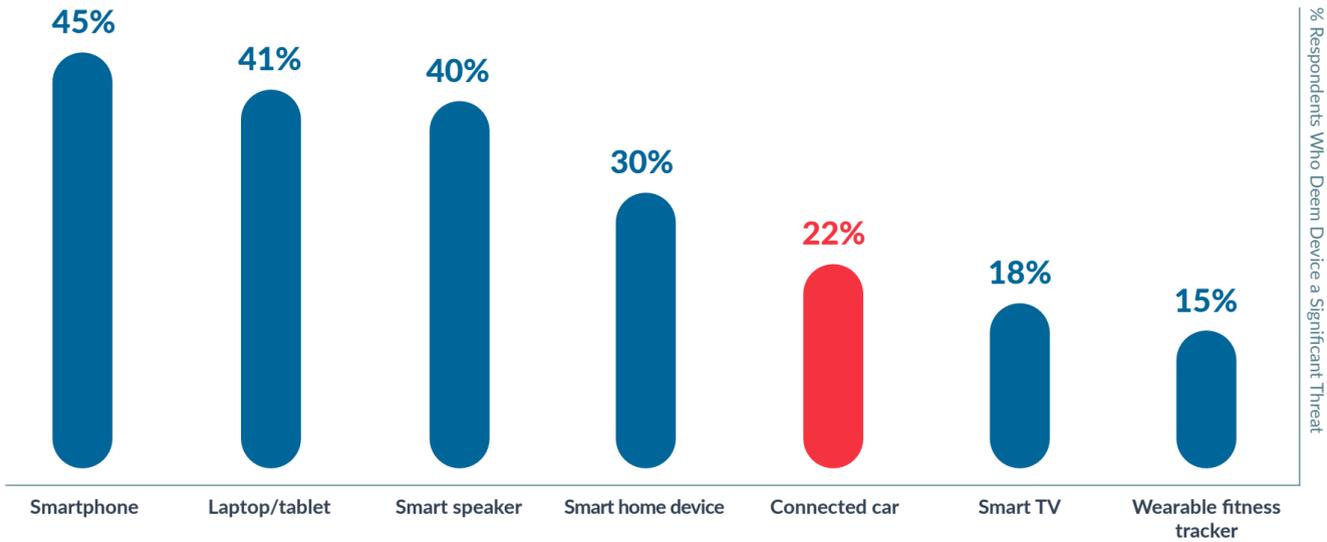
70%

of people who own a connected car have used vehicle smartphone integration in the past year.

Perceived Data Security Threat of Connected Cars

● Minimal threat ● Moderate threat ● Significant threat

All respondents

42%	35%	22%

18–29 year-olds

54%	28%	18%

Perceived Data Security Threat Across Connected Devices

% Respondents Who Deem Device a Significant Threat

Smartphone	Laptop/tablet	Smart speaker	Smart home device	Connected car	Smart TV	Wearable fitness tracker
45%	41%	40%	30%	22%	18%	15%

Pop Quiz!

We tested drivers on automotive data security, including best practices and general awareness. Here's how they did.

49% The average score among all respondents

53% The average score among owners of connected cars

See How You'd Do

The Disconnect Among Connected-Car Owners

Even those with the latest in automotive technology (i.e., connected-car owners) aren't aware of their vehicles' data security risks. Here are some of the most common misconceptions we uncovered.

✕ **46%** weren't aware of data security best practices in connected cars.

✕ **61%** didn't know that a hacker can hijack control of a connected car's steering wheel or brakes.

✕ **33%** didn't know that key fobs are vulnerable to hacking.

✕ **65%** thought auto manufacturers are legally required to notify owners of data security updates. (FYI, they're not.)