



How to **avoid**
a 'relay attack'
on your car



The Insurance Crime Bureau recently reported an increase in car theft, particularly of newer model sports utility vehicles (SUVs) that have keyless entry and ignition technology, by syndicates using a method known as "relay attack".

How a *relay attack* works

A relay attack works by essentially using a device which acts as a "receiver" to tap into the key fob (also known as a hardware token that provides on-device, one-factor authentication for access to a system or device like a car) signal.

One thief lurks outside your home or office with a device that acts like a receiver to "trap" the signal from your key. He/she then transfers that signal to his/her partner with a similar device, next to your car, relaying the key's signal to unlock the car.

If held close to the target vehicle, this device allows criminals to unlock the vehicle, start the engine and drive off with your car.

How is this *different from signal-jamming*?

Signal-jamming prevents the car from being locked whereas this new device allows perpetrators to copy the signal, allowing them to unlock, start the car and drive away with it.

How to *avoid a relay attack*

The easiest way to avoid a relay attack is to:

- deactivate the keyless entry (key fob) functionality when in a high-risk area if possible.
- Store the key in a special key pouch that blocks the signal.
- keeping the key far away from the vehicle when not in use.

