Scams

Gary Friedman of Sunrise Ct. and a member of the Safety and Security Committee sent this article from Car and Driver to me and I thought it was worth passing on.

“We got an e-mail warning us about thieves hacking into keyless-entry systems to unlock cars. According to the scenario in the e-mail, thieves lurk near the victim's car with equipment that intercepts and steals the transmitted code from the key fob as the driver presses the lock button. Then, they use their equipment to unlock your car using the stolen code. All together now: Donkey show! According to the lock specialists at Ford, each keyless-entry transmitter has a transmitter identification code (TIC) that is programmed and, therefore, linked to the vehicle. But even if thieves manage to mimic the TIC, the unlocking/locking process is even more complicated. Here's how it works: To issue an unlocking/locking action, the transmitter sends a request to the receiver/control module in the car. With the request, the transmitter also sends a new code sequence and TIC to the receiver. To issue an unlock/lock command, the code sequence and TIC sent by the transmitter must be one that hasn't been used before and the next, or one of the next few, in a planned sequence. This is what is known as a rolling code. And there aren't just a lot of possible codes; there are a whole butt load of them - 4.8 million/billion combinations. So even if thieves did manage to steal the TIC *and* the code sequence from the transmitter the chance of stumbling upon that crucial next code is one in 4.8 million/billion. Good luck with that.” Also, you cannot send radio waves over the telephone, so that claim about having someone holding your extra key fob to the phone and unlocking your doors is not true.

Bob Mattsson