Anti-Theft Measures

A Layered Approach is Most Effective

Use Faraday Pouches or Containers: These special pouches block RF signals, preventing fobs from emitting detectable transmissions. A Faraday cage or box at home can secure key fobs within a shielded zone.

Disable Passive Keyless Entry: Some vehicles allow owners to disable the keyless entry feature entirely when not in use (refer to the user manual).

Distance from Entry Points: Store fobs far from windows, doors, or garage walls to reduce the likelihood of signal detection or relay attacks.

Reprogram Key Fobs: If you feel your vehicle key fob has been compromise, some manufacturers offer services to update or reprogram your fob to prevent vulnerabilities.

Additional Security Layers: Ensure your vehicle has secondary anti-theft measures such as immobilizers or after-market audible alarms that are compatible and safe for your vehicle. Criminals do not want to spend time problem-solving deterrents. Having visible anti-theft device deterrents can improve the probability that the criminal will not proceed. Here are some examples.

- ***Digital Anti-theft Systems:*** IGLA Alarm, OBD Block; Compustar Pro T13, Pro R5, CS7900-AS
- ***Steering Wheel Locks***: The Club 3000; Tevlaphee Sterring Wheel to Seatbelt Lock
- ***Wheel Lock Immobilizers:*** Tevlaphee; Cartman; Turnart
- ***Gas Throttle Controllers:*** Pedal Commander Anti-Theft; Soler Performance
- ***Brake Locks:*** Tevlaphee Pedal Lock; Unbreakable Autolock

Dear Residents of the Seven Isles Community,

To effectively manage and diminish the potential for criminal activities, SIG 9 Global has implemented a range of strategies aimed at discouraging unlawful behavior within the Seven Isles Community, particularly regarding instances of vehicle theft. Nonetheless, it is crucial for residents to engage in proactive and vigilant practices that reduce risk and address identifiable vulnerabilities, thereby reinforcing the effectiveness of any additional security measures. Vehicle theft rings actively target areas where critical errors—such as unsecured vehicles or key fobs left inside—facilitate quick, low-resistance crimes with minimal detection. Empirical evidence suggests that once these offenders achieve success in a neighborhood, they are likely to return, perceiving the area as a reliable target for similar opportunities. Furthermore, these criminal organizations use advanced technological methods such as relay hacking, key cloning, and address theft, alongside pre-planned strategies and observations of human error, to exploit gaps in security systems. However, the presence of key fobs inside vehicles is among the most common enablers of vehicle theft, particularly in vehicles equipped with keyless entry and start systems. To mitigate these risks, implementing layered physical and technological security measures is essential. These measures include the secure storage of key fobs in RFID-blocking devices (e.g., Faraday pouches), confirming vehicles are locked, and installing enhanced security features such as aftermarket alarm systems, steering wheel locks, immobilizers, hidden vehicle trackers, and PIN-protected operations.

Please remember that a thorough and methodical approach to crime mitigation requires consistent practices, integration of effectively layered deterrents and collaboration. By addressing vulnerabilities and enhancing the complexity of crimes that may arise as opportunities, residents can markedly reduce the likelihood of becoming victims. Moreover, fostering collaborative security mitigation as a community is detrimental in lowering the probability of Seven Isles being perceived as a target area for criminal activity.

Let's work together to maximize safeguarding the Seven Isles Community.

SIG 9 Global

Supporting Research

Linning et al. (2024) state "to fully explain crime patterns, we need to account for two processes: how crime opportunities are created and how offenders discover crime opportunities" (p. 2). Furthermore, Welsh et al. (2017) highlight Clarke's (1992) notion that "situational crime prevention has been defined as 'a preventive approach that relies, not upon improving society or its institutions, but simply upon reducing opportunities for crime.' This is brought about by modifying or manipulating the physical environment in order to directly affect offenders' perceptions of increased risks and effort and decreased rewards, provocations, and excuses" (p. 150) compliments Linning's et al. (2024) assertions.

Linning, S. J., Bowers, K., & Eck, J. E. (2024). Crime radiation theory: The co-production of crime patterns through opportunity creation and exploitation. *Crime Science, 13*(1), Article 32. https://doi.org/10.1186/s40163-024-00234-6

Welsh, B. C., Zimmerman, G. M., & Zane, S. N. (2017). The centrality of theory in modern day crime prevention: Developments, challenges, and opportunities. *Justice Quarterly*, *35*(1), 139–161. https://doi.org/10.1080/07418825.2017.1300312

The information provided below may be beneficial in establishing strategies to effectively manage and minimize the risk of vehicle theft incidents.

Practices and Methods of Vehicle Theft Exploitation

Exploitation of Key Fob Vulnerabilities: A significant proportion of rapid vehicle thefts involve weaknesses in keyless systems. Criminals may detect fobs left inside vehicles or even proximity to the car. Organized theft rings use systematic targeting and pre-planning techniques that often scout neighborhoods, or parking areas to identify patterns and weaknesses. Here are methods they can use:

Exploiting Human Error: In a high proportion of cases, an owner inadvertently leaves the fob inside a car which offers criminals the easiest scenario. Once they find the car, they can access and start it in seconds, requiring no additional tools.

Scanning for Active Key Signals: Criminals may patrol public spaces (e.g., residential communities, garages, parking lots) with tools (e.g. Radio Signal Scanner or RFID signal detector**)** that scan for signals from fobs that are active or left in vehicles. ***Detection Range:*** Depending on the sophistication of the device, the scanning range can vary from a few feet to hundreds of meters. Some devices include amplifiers to increase the effective range. This allows them to methodically locate vulnerable targets swiftly and in higher numbers.

Keyless Relay Attacks (Relay Hacking): Thieves use a pair of devices (relay amplifiers) to intercept and extend the low-frequency signal emitted by a key fob. One device is placed near the fob (e.g., through a car owner's window or front door at their home), and the original key fob is near the car. This "relays" the signal, tricking the vehicle into unlocking and starting.

RF spectrum analyzers or **RF signal sniffers**: These off the shelf RF detection tools are designed to troubleshoot wireless systems or locate RF sources. Unfortunately, these tools can be modified and misused by criminals to exploit keyless entry systems in cars.

Key Fob Cloning and Theft of Owner Information: Targeted vehicle thefts sometimes stem from skimming personal data, which can provide thieves with address information to locate vehicles. Methods include:

Use of Key Cloning or Skimming Devices: Thieves can intercept signals to clone fob credentials during brief contact with the owner (e.g., at a valet, mechanic, or fuel station) using proximity skimming devices. This can give them access to the car later if they can obtain the owner's residence or place or work by data searches, following the victim, or data theft.

Stealing Addresses from Glove Boxes or Dash Systems: Some criminals gain access to the vehicle first and collect personal information stored in onboard systems or documentation (e.g., insurance cards or vehicle registration) to identify where the vehicle is regularly kept, enabling a follow-up theft.

OBD Port Reprogramming: Once inside the vehicle, thieves use portable devices like a diagnostic key programmer plugged into the On-Board Diagnostics (OBD) port to reprogram a blank key and start the vehicle.

Jamming Devices: Criminals sometimes use signal jammers to block remote key fob locking signals, leaving cars unlocked.