

Protect Your Automobile

A 90-minute, discussion-led session kit for dealerships

Habits

- Keep guest Wi-Fi separate from finance, service, and the parts system.
- Do not take a credit application on guest Wi-Fi.
- Call back before a down payment or a parts payment changes accounts, using a number you already trust.
- Set the car's Wi-Fi password with the buyer before delivery, and remove phones paired on the test drive.
- Treat a lost key fob or app login like a lost key.
- Match the person, the ID, and the application before the loan is sent.

Red flags

- A guest Wi-Fi page that asks for a password or a credit application
- A last-minute change to where a down payment or a parts invoice should be paid
- A sender address one letter off from the lender or the supplier
- A car hotspot that uses the office password
- A phone still paired to a car that is ready for delivery
- A part, key, or module that does not match the VIN

First hour

1. **Bank.** The buyer or the dealership calls the bank now and asks to stop or recall the payment.
2. **Report.** File at ic3.gov with the transaction details.
3. **Notify.** The general manager, the lender, and the supplier you already use.
4. **Contain.** Take down a Wi-Fi page you did not post, reset the changed account, and hold any part that does not match the VIN.

Figures on the session page are FBI IC3 2025 totals for those crime types, not a dealership-only count. File a report at ic3.gov.