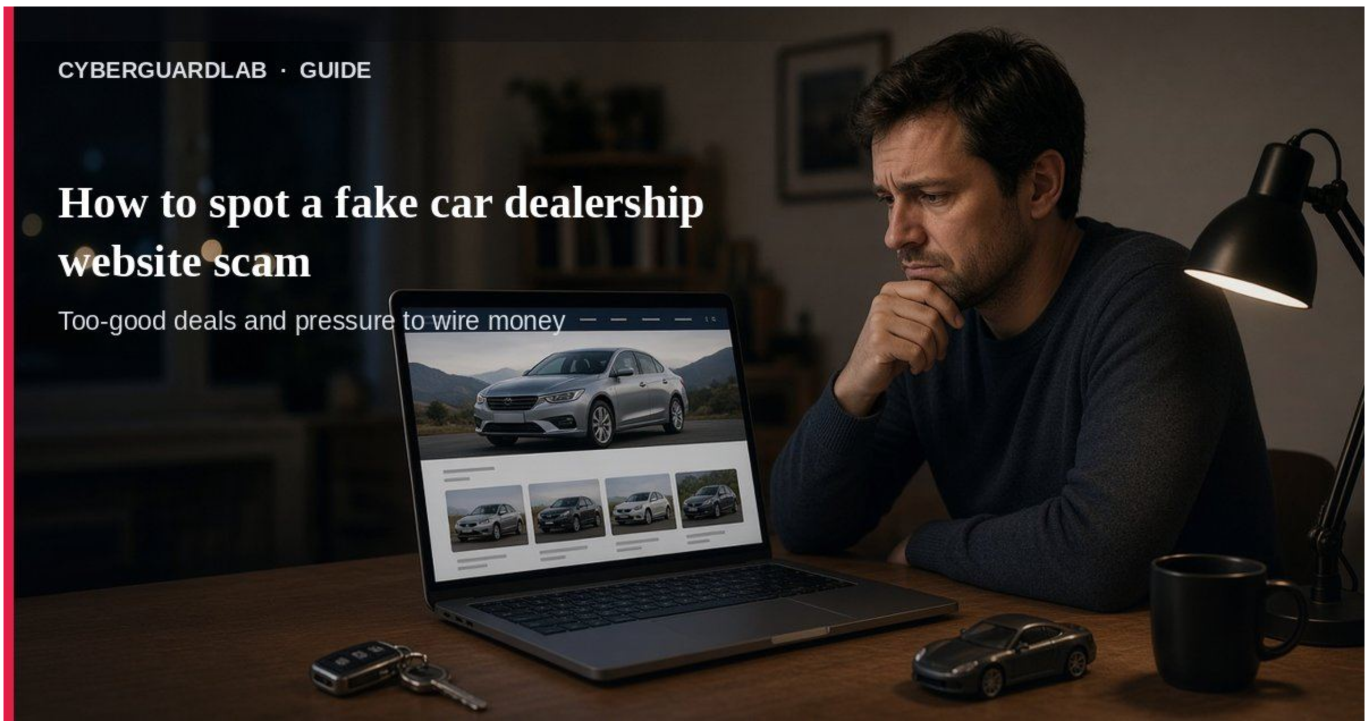
# How to spot a fake car dealership website scam

https://cyberguardlab.com/blog/fake-car-dealership-website-scam

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.




A fake car dealership website scam is when criminals clone a real dealer's site - logos, inventory photos, even fake reviews - so you pay up front for a car that never exists. The FTC's September 2026 consumer alert says buyers show up at the real lot and learn there is no order and no vehicle. This guide is about bogus online car-dealer stores, not phishing emails in general, fake checks, or QR parking codes. You do not need to buy antivirus to refuse a wire-only deposit.

## 1. How the scam usually works

From the FTC alert:

* Cloned websites - Scammers copy a real dealer's branding and listings, sometimes with AI, including photos and fake testimonials.
* Too-good inventory - Rare muscle cars or hard-to-find classics are used as bait.
* Polished sales script - Detailed buying steps and flexible "return policies" to build trust.
* Upfront payment - Especially pressure to pay by wire transfer only before you see the car.
* No car at the real lot - You arrive and the real dealership has no record of you or your payment.

## 2. What to do before you send money

FTC protection steps:

* Search the dealer name with "scam," "review," or "complaint." Negative hits are a red flag.
* Remember glowing reviews can be faked - especially if scammers are impersonating a real brand.
* Ask to see the car and the dealership in person. If they won't, pump the brakes.
* If the car is far away, insist on a mobile inspection you hire yourself. If they refuse, walk away.
* Refuse wire-only upfront payments. FTC: walk away if the dealer insists on an upfront payment by wire transfer only.
* Pay only through channels you initiated with a dealer you verified independently - not a cold link from an ad or text.

## 3. First-hour checklist if you already paid

* Contact your bank or wire provider immediately and say it was a scam.
* Save the website URL, screenshots, emails, texts, and payment receipts.
* Call the real dealership (number from a known directory, not the fake site) to confirm they never sold you that car.
* Report at ReportFraud.ftc.gov.
* If you also shared passwords or opened a shady file on a PC, change passwords and run your existing Windows security tools - buy-nothing/Defender is enough for many homes.

## 4. Household habits that cut risk

* Never buy a car sight-unseen from a site you found only through a sponsored ad or random DM.

* Type the dealer name yourself and confirm the physical address matches a real lot.
* Treat "wire today or lose the car" pressure like any other FTC scam tell.
* Keep phone and email on MFA so a hacked inbox is harder to use for follow-up fraud (see turn on 2FA and CISA MFA).
* Teach teens in the house the same "see it in person or hire your own inspector" rule for private-party car ads.

## FAQ

### How do I spot a fake car dealership website scam?

A site that looks identical to a real dealer, pushes rare cars, and demands wire-only upfront payment - while refusing an in-person visit or independent inspection - matches the FTC's alert pattern.

### What if the reviews look real?

FTC notes that when scammers impersonate a real dealership, you may still find glowing reviews. Still require seeing the car or using your own inspector.

### Is Microsoft Defender required here?

No. The core problem is paying a fake dealer. Defender helps only if you also clicked malware on a PC - see Is Microsoft Defender enough?.

### How is this different from a normal online car listing?

Legitimate sellers let you verify the car and the business. Cloned-site scams sell the website, then vanish after the wire.

### Where do I report it?

ReportFraud.ftc.gov.

## If you still want a paid suite

Avoiding a cloned dealer site does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is verifying the lot in person and refusing irreversible wires. If the household later wants multi-device paid protection, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

## Sources

* Scammers are spoofing car dealership websites: What you need to know (FTC)
* How To Avoid a Scam (FTC)
* ReportFraud.ftc.gov (FTC)
* Learn where to report a scam (USAGov)
* Turn On MFA (CISA)

## Also read

* How to spot a phishing email
* How to spot a fake check scam
* How to spot a QR code scam
* How to spot a gift card scam
* Check a download before opening an EXE