

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a fake online store before you buy

[Read online: https://cyberguardlab.com/blog/fake-online-store-scam](https://cyberguardlab.com/blog/fake-online-store-scam)

Published October 14, 2026 | Updated October 14, 2026

Short answer

A fake online store is a website that copies the look of a real retailer or invents a "brand outlet," takes your card or payment-app money for a deeply discounted product, and then ships nothing, a knockoff, or something you never ordered. Most people meet these sites through an ad or sponsored post in their social feed, not through a search. The Federal Trade Commission's April 27, 2026 alert says shopping scams were the most reported scam that started on social media, and that most people who reported one said the item never arrived. The FTC's August 26, 2025 alert adds that some of these copycat sites are built to collect your Social Security or bank account number, not just your payment. This guide covers the checkout decision on an unfamiliar website: who is really selling, whether the price makes sense, and how you are being asked to pay. CyberGuardLab writes these explainers independently. A few product pages on this site earn affiliate commissions, and that can influence which tools we list; every check below is free, and the only paid links sit in a clearly labeled section near the end.

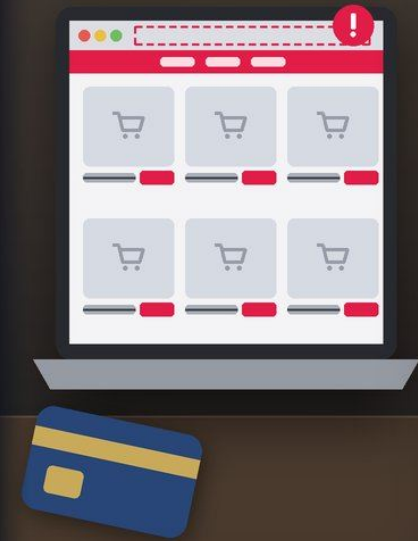
Advertising disclosure: CyberGuardLab is an independent comparison site. We are not TotalAV, Norton, Bitdefender, McAfee, or Avast. If you buy through our links, we may earn a commission, which can affect ranking and placement.

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.

CYBERGUARDLAB · GUIDE

How to spot a fake online store before you buy

Check the seller before a too-good deal gets your card.



Short answer

Before you pay an unfamiliar store, close the ad and look the seller up yourself: search the store name or web address with "scam," "complaint," or "review," and compare the price with what known retailers charge. A padlock or "https" proves only that the connection is encrypted, not that the business is real. Pay with a credit card so you can dispute the charge, and walk away from any seller that insists on gift cards, wire transfers, payment apps, or cryptocurrency.

Where fake stores find shoppers

The FTC and FBI describe the same path again and again:

Paid link

Norton 360 | [See the Norton first-year offer](#)



[See the Norton first-year offer](#)

Offer page: <https://cyberguardlab.com/norton> Hop: <https://trysecurities.com/offer/norton?dtm=gg&cid=>

- * A sponsored post promises a big name at a tiny price. The FTC's May 2024 alert says social feeds are flooded with ads offering steep discounts on brand-name and luxury items, and that scammers often impersonate real companies in those ads. Its December 2023 holiday alert names Facebook and TikTok as places where these copycat ads run.
- * The ad's brand is not the seller. The August 2025 FTC alert warns not to assume the seller is the company named in the ad, and to look closely to see who the seller really is before clicking.
- * The site looks finished, padlock included. The FTC's Online Shopping guide notes that "https" means a site is encrypted but does not mean it is legitimate, because scammers know how to encrypt sites too.
- * Checkout steers you toward money that is hard to claw back. The same guide says to never buy from online sellers who insist on gift cards, wire transfers through companies like Western Union or MoneyGram, a payment app, or cryptocurrency. The FBI's holiday shopping guidance says money sent by money transfer company, prepaid card, or bank-to-bank wire is virtually impossible to recover.
- * After payment, the order stalls. The April 2026 FTC alert says most people who reported a social media shopping scam never got the item, and others received a knockoff or something different from what they ordered. The FTC's report on undelivered online orders describes sellers who blamed shipping delays and then stopped answering.

Fake-store warning signs

What you notice | What the official guidance says | What to do

Brand-name item at a fraction of the usual price | FTC August 2025: if the ad's price is much, much lower than elsewhere, it is probably a scam | Check the same model number at retailers you already know

The store name in the address bar differs from the brand in the ad | FTC August 2025: do not assume the seller is the brand the ad names | Type the brand's real site yourself and look for the deal there

No clear return policy, shipping time, or way to contact the company | FTC May 2024: if you cannot find warranties, returns, shipping times, and contact details, walk away | Close the tab before entering card details

Checkout only takes gift cards, wires, payment apps, or crypto | FTC Online Shopping guide: only scammers demand those methods; they make refunds hard | Do not pay; report the site

Glowing reviews that all sound alike | FTC Online Shopping guide: some reviews and ratings are fake; do not rely on stars alone | Read reviews on several independent sites, not only the store's own page

Real retailer vs copycat storefront

Question | Copycat storefront | Retailer you reached on your own

How you got there | Tapped a sponsored post, giveaway, or unfamiliar link | Typed the address, used a saved bookmark, or opened the official app

Who the seller is | Unclear, or a new name dressed in a famous brand's logo | Named company with a findable track record and contact details

Payment options | Pushes gift cards, wires, crypto, or a direct payment-app transfer | Accepts credit cards, which the FTC says give you the best protection

After you order | Vague delays, no tracking, then silence | Order confirmation and a tracking number you can follow

How to spot a fake online store before you buy

Work through these six checks while the cart is still open.

- * Leave the ad and find the store yourself. The FTC's December 2023 alert says to go to the company's website through a page you know is official, not the link in the ad. If the famous brand's real site does not show the same deal, treat the ad's store as an impostor.
- * Search the store's name and web address with "scam," "complaint," or "review." The FTC's May 2024 alert says to do that search in a search engine rather than inside the social media app, so you see what other shoppers have reported. Its Online Shopping guide adds that reviews should come from several independent sites, because some ratings are fake.
- * Compare the price with what known sellers charge. Note the manufacturer and model number, then check retailers you already trust. The FTC's Online Shopping guide warns that expensive brand-name items offered at bargain prices could be counterfeit or stolen.
- * Read the shipping, return, and contact details before you type a card number. The FTC's May 2024 alert says to check warranties, return policies, shipping times, and how you would reach the company; if that information is missing, walk away. You can also paste the address into Google's Safe Browsing site status page. A warning there is a clear stop sign, but a clean result only means Google has not flagged the site as dangerous, so it does not prove the store is real.
- * Pay by credit card, never by gift card, wire, payment app, or crypto. The FTC's Online Shopping guide says a credit card gives you the best protection if something goes wrong and lets you dispute charges for items you never got. The same guide says only scammers insist on gift cards, wire transfers, payment apps, or cryptocurrency.
- * Keep the paper trail until the package arrives. The FTC's Online Shopping guide lists what to save: the company name and website, what you ordered and paid, the return policy, the shipping promise, and every email or text. The FBI's holiday shopping guidance says to always get a tracking number. Those records are what your card issuer and the FTC will ask for if the order never comes.

If the order never shows up

- * Ask the card company to dispute the charge. The FTC's Online Shopping guide says to call right away and send a letter that reaches the card company within 60 days of the date it mailed the first bill showing the charge. This site's dispute a fraudulent credit card charge guide walks through the call and the letter.
- * If you paid through a payment app or bank transfer, the FBI's 2023 holiday shopping PSA says to contact your financial institution right away to try to stop or reverse the transaction and to report the activity to the payment service you used.
- * If you typed card details into a site you now doubt, follow what to do in the first hour after credit card fraud so the card can be replaced before more charges land.
- * If the checkout also asked for a Social Security or bank account number, the FTC's August 2025 alert points to IdentityTheft.gov (Report identity theft).
- * Report the store at ReportFraud.ftc.gov (How to report a scam to the FTC) and file a separate complaint at IC3.gov, which the FBI asks shoppers to use as quickly as possible.

Free habits that keep copycat stores out of your cart

- * Shop famous brands through their own apps or a bookmark you saved, and treat a social ad as a reminder to check that official site, not as the place to buy.
- * Turn on stronger phishing and dangerous-site warnings in your browser (Turn on enhanced Safe Browsing in Chrome).
- * Keep one credit card for online shopping so a bad checkout touches only one account, and turn on purchase alerts in the card's official app.
- * Never "unlock" a deal by paying a different way than the site first advertised. A store that suddenly wants a gift card or a Zelle or Cash App transfer is telling you what it is.
- * Tighten who can see your social media posts and contacts; the FTC's April 2026 alert says that gives scammers less to work with.

What this page is not

This guide is about a stand-alone website that poses as a store, usually reached from an ad, and the moment before you pay it.

Purchases inside a social app's own shop or a live stream are covered in [How to spot a TikTok shop or live-stream scam](#). Person-to-person listings and local pickups are in [How to spot a Facebook Marketplace scam](#). Big-ticket fake vehicle sites have their own checklist in [How to spot a fake car dealership website scam](#), and deposits for animals that never arrive are in [How to spot a pet adoption or puppy deposit scam](#). A box that arrives without any order is a different problem, covered in [What to do if you get a package you didn't order](#). If the lure was an email that pretends to be a retailer's receipt or account notice, start with [How to spot a phishing email](#). Disputes with a real store over late shipping or returns are consumer complaints rather than scams, and nothing here is legal advice beyond the FTC and FBI pages cited below.

Optional paid security suites

You do not need software to catch a copycat store; the checks above are enough. If you were already planning to buy device protection, these on-site comparison pages are the only paid links in this guide:

- * Norton plans: suites that pair device protection with identity features on higher tiers ([paid link](#); note the renewal price).
 - * Bitdefender plans: worth a look if independent lab test results matter most to you ([paid link](#)).
 - * TotalAV plans: a household option to compare on device count and first-year price ([paid link](#); read what renews).
 - * McAfee plans: one bill that covers several phones and computers ([paid link](#); confirm the device limit).
 - * Avast plans: an option if your household already uses Avast and wants to stay with it ([paid link](#)).
- Buying none of these is a perfectly good choice.

FAQ

Does a padlock or "https" mean the store is safe?

No. The FTC's Online Shopping guide says the "s" in https means the connection is encrypted, but it does not mean the site is legitimate, because scammers can encrypt their sites too.

The ad used a famous brand's logo. Isn't that proof it's real?

No. The FTC's August 2025 and May 2024 alerts both say scammers impersonate real companies in social media ads. Go to the brand's official website through a page you already know and check whether the same deal exists there.

How can I check a store I've never heard of?

Search its name and web address with "scam," "complaint," or "review" in a search engine, as the FTC recommends, and read reviews on several independent sites. You can also check the address on Google's Safe Browsing site status page, keeping in mind that a clean result is not a guarantee.

Which payment method protects me most?

A credit card. The FTC says it gives you the best protection and lets you dispute charges for items you never received. The FTC also says only scammers insist on gift cards, wire transfers, payment apps, or cryptocurrency.

How long should I wait before I decide the order isn't coming?

The FTC's Online Shopping guide says sellers must ship as promised in their ads, and if no time was promised, within 30 days of getting your order and payment. If the promised date passes with no tracking and no answers, contact your card company about a dispute rather than waiting for more excuses.

I paid and nothing came. What now?

Dispute the charge with your card company, keeping the FTC's 60-day letter deadline in mind, or contact your bank or payment service right away if you paid another way. Then report the store at ReportFraud.ftc.gov and IC3.gov. If you also gave a Social Security or bank account number, go to IdentityTheft.gov.

Sources

- * Online Shopping (FTC Consumer Advice)
- * That social media ad with super low prices on well-known brands could be a scam (FTC Consumer Advice, Aug 26, 2025)
- * Spot an ad on social for a low, low price on a brand name product? Think twice (FTC Consumer Advice, May 2024)
- * Last-minute shopping? Three ways to spot rip-offs (FTC Consumer Advice, Dec 2023)
- * How to spot the top scams that started on social media (FTC Consumer Advice, Apr 27, 2026)
- * Scams in online sales: when orders don't arrive (FTC Consumer Advice)
- * Avoid Holiday Shopping Scams (FBI)
- * 2023 Holiday Shopping Scams (FBI IC3 PSA)
- * Safe Browsing site status (Google Transparency Report)
- * ReportFraud.ftc.gov
- * IdentityTheft.gov
- * Internet Crime Complaint Center (FBI IC3)

Also read

- * Fake delivery text scams
- * Fake ticket resale scams
- * Amazon Prime renewal scams
- * Fake refund overpayment scams