CyberGuardLab

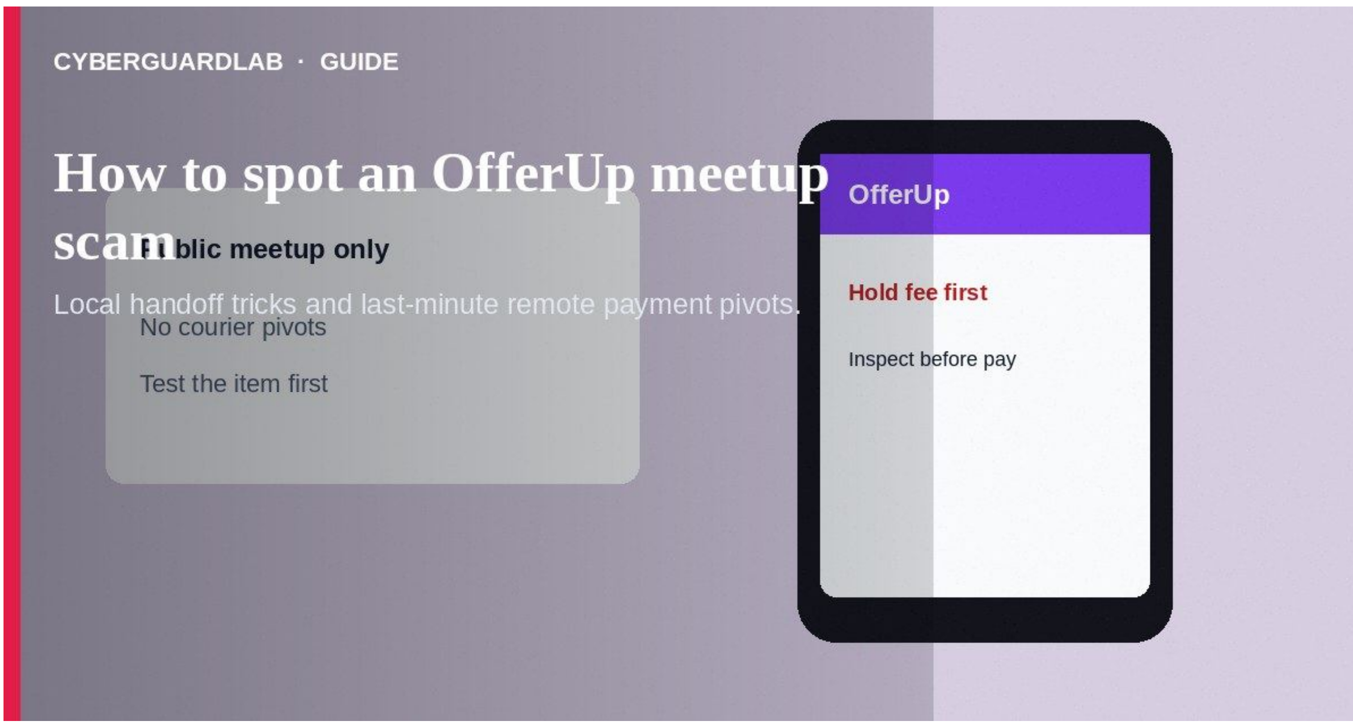
Household antivirus, explained

cyberguardlab.com

How to spot an OfferUp meetup scam

https://cyberguardlab.com/blog/offerup-meetup-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.



An OfferUp meetup scam targets local buy-and-sell deals: fake buyers who never show, sellers who demand payment before you inspect the item, switcheroo goods, or "shipping agents" who cancel the meetup and push remote payment. Do not pay before you see and test the item in a safe public place. Do not share one-time codes or remote-access apps with "OfferUp Support." If you already paid and got nothing, stop contact, save chat logs, and report through OfferUp and the FTC.

This guide focuses on in-person and last-minute remote pivots on local marketplace apps-not eBay seller email impersonation after an online auction. Link caution overlaps with phishing emails. Instant-pay pressure overlaps with Zelle and Cash App payment scams. No software purchase required.

1. How OfferUp meetup scripts work

A listing for a phone, bike, console, or furniture looks local. The seller asks for a Venmo/Zelle hold before meetup, or the buyer asks you to ship after a partial payment. At meetup, some swap a working demo for a broken unit in the box. Others cancel minutes before and insist you pay a courier who never arrives.

* Deposit-before-inspect - Hold fees to "reserve" an item you have not seen.
* Bait-and-switch handoff - Demo unit works; the boxed unit does not.
* Courier pivot - Local pickup becomes a remote shipping-agent payment.
* Fake support - Cold calls after you message someone demand codes or screen sharing.

2. Red flags before you pay

Cue	Likely legitimate	Likely scam
Meetup	Public place, daytime, item present to inspect	Deposit required before you see the item
Payment timing	Pay when you accept the item in person	Pay a shipper or agent who never meets you
Account signals	Ratings and history you can review in-app	Brand-new account, stock photos only, rushes you
Chat location	Stays in OfferUp messaging	Forces WhatsApp/text and deletes the listing
Item check	Lets you power on, verify serial, test functions	Sealed box you must not open, or bait-and-switch
Support	You open OfferUp Help yourself	Cold call asking for codes or screen sharing

3. Safer habits (buy-nothing)

* Meet in a public, well-lit place; bring a friend when possible.
* Inspect and test before paying. For phones and laptops, confirm they are not activation-locked.
* Prefer paying at the meetup for what you are holding-not advance deposits to strangers.
* Decline shipping pivots from people who advertised local pickup only.
* Keep chats in the app so you have a record; report suspicious users in-app.

* Ignore OfferUp Support calls; open help from the official app or site.

4. If you already paid

* Stop further payments. Screenshot the listing, profile, chat, and payment confirmation.
* Report the user through OfferUp's official reporting tools.
* Contact your bank or payment app's fraud team right away (FTC if you were scammed).
* If you shared card or login details on a fake page, change passwords and enable two-factor authentication.
* File a report at ReportFraud.ftc.gov.
* If you installed remote tools or opened odd links, change passwords and ignore recovery callers.

FAQ

Is paying with Cash App at a meetup safe?

It can still be irreversible. Inspect first, confirm the person matches the account story, and never send extra "fee" payments afterward.

The seller wants a small hold fee so they do not sell to someone else.

That is a common loss pattern. If you cannot see the item, walk away.

How is this different from an eBay impersonation scam?

eBay impersonation often uses email/SMS to hijack an online purchase thread. OfferUp meetup scams center on local handoff tricks and last-minute remote payment pivots.

Can police help if I met in their parking lot?

Some departments promote safe-exchange zones. Still report fraud with your evidence; outcomes vary by case.

What if the buyer's cashier's check needs days to clear?

Treat unsolicited checks as high risk. Wait for true clearance under your bank's guidance-or decline and use cash you can verify.

Do I need paid antivirus to avoid an OfferUp meetup scam?

No. Inspect-before-pay habits and refusing remote pivots are enough. Buy-nothing is valid.

If you still want a paid suite

Avoiding a OfferUp meetup scam does not require paid antivirus. Careful habits and official support paths are a valid buy-nothing stack. If you want multi-device paid protection later, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* Online Shopping Tips (FTC)
* ReportFraud.ftc.gov
* IdentityTheft.gov
* Phishing Scams (FTC)

Also read

* How to spot an eBay seller impersonation scam
* How to spot a Zelle or Cash App payment scam
* How to spot a phishing email
* How to spot a fake check scam
* How to report a scam to the FTC