CyberGuardLab

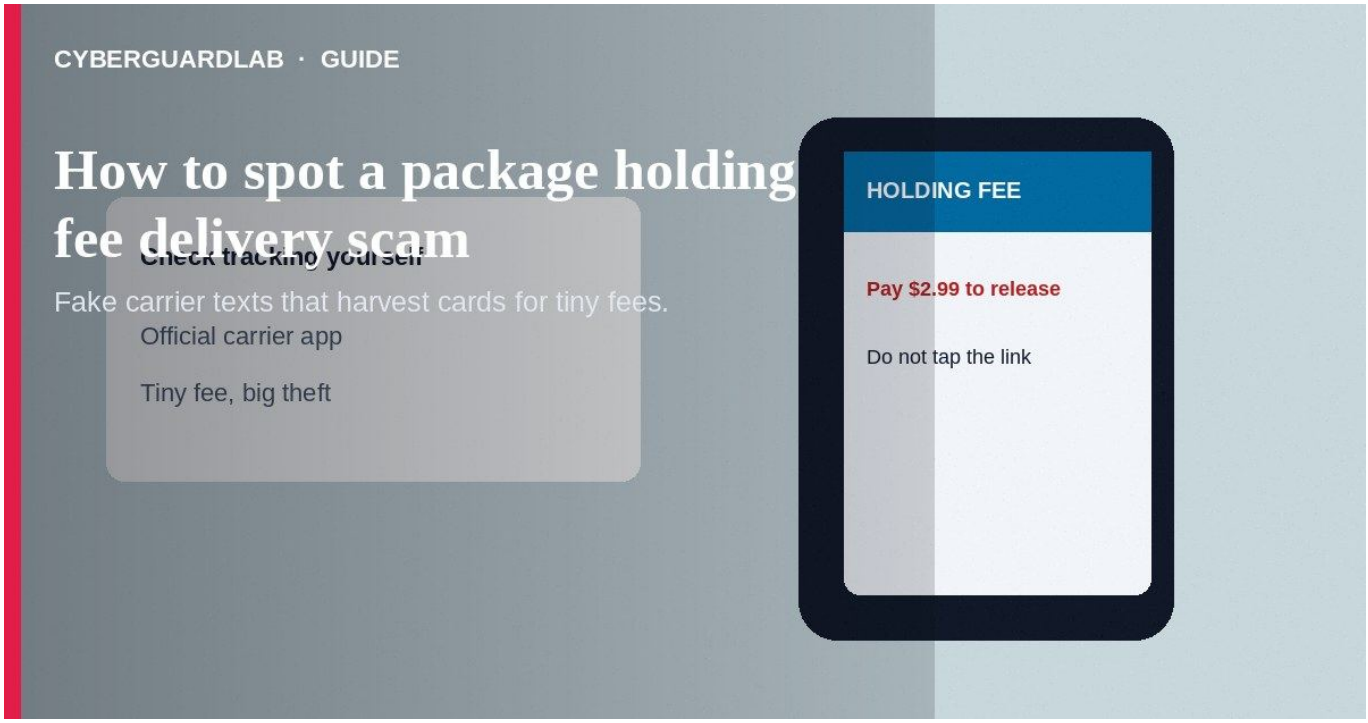
Household antivirus, explained

cyberguardlab.com

How to spot a package holding fee delivery scam

https://cyberguardlab.com/blog/package-holding-fee-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 package holding fee delivery scam texts or emails that a parcel is delayed, seized, or waiting at customs-and you must pay a small holding, redelivery, or postage-due fee through a link. The link is usually phishing. Do not tap it. Do not pay with gift cards or crypto for a mystery package. If you already entered card data, call your bank, change passwords, and report to the FTC.

This guide covers fake delivery-fee messages-not fake Amazon customer service phone calls about account charges or remote-access refunds. Timing often follows a real purchase so the story feels plausible-similar phishing patterns appear in how to spot a phishing email and fake delivery text scams. No software purchase required.

1. How package holding fee scripts work

SMS messages claim USPS, UPS, FedEx, DHL, or Amazon Logistics need $1-$5 (or more) to release a package. Short links lead to pages that harvest card numbers, addresses, and sometimes ID uploads. Emails use tracking numbers that look real but are random.

* Postage-due bait - Tiny fee to release a package that may not exist.
* Customs or warehouse holds - Urgency to pay before the parcel is destroyed.
* Credential harvest - Pages that look like carrier portals (FTC phishing guidance).
* Follow-up calls - Voice calls still push payment links or codes.

2. Red flags before you tap

Cue | Likely legitimate | Likely scam

How you pay postage due | Carrier instructions you verify on the official site/app after you look up tracking yourself | Cold text with a pay link

URL | Exact carrier or retailer domain | Misspelled domains, odd short links, strange subdomains

Amount and urgency | Matches a real shipping exception you can see in tracking | Pay in 2 hours or package destroyed

Payment method | Normal card checkout on an official page | Gift cards, crypto, wires

Data asked | Minimal delivery confirmation details | Full SSN or photo ID upload for a $3 fee

Account path | You open the retailer/carrier app yourself | Message pretends to be support and asks for OTP codes

3. Safer habits (buy-nothing)

* Do not tap the link. Delete or report the text as junk.
* If you expect a package, open the carrier or store app yourself and check tracking (USPS.com as a starting point for USPS).
* Use official redelivery tools from the carrier's real website.

* Never pay a holding fee with gift cards.
* Share the sample with household members who receive lots of deliveries.
* If a caller claims to be Amazon account support rather than a fee link, see fake Amazon customer service calls.

4. If you already paid or typed data

* Contact your bank or card issuer to watch for charges and replace the card if needed (FTC if you were scammed).
* Change passwords for email and shopping accounts; enable two-factor authentication.
* Save screenshots of the message, URL, and any pages.
* Report at ReportFraud.ftc.gov; report phishing to the carrier if they publish a channel.
* If you uploaded ID images, review steps at IdentityTheft.gov.
* Ignore callers who promise to "clear" the fee for another payment.

FAQ

I really am waiting on a package. Could the text be real?

Possibly rare legitimate notices exist, but safe practice is to ignore the link and check tracking yourself on the official app.

The tracking number format looks right.

Scammers generate realistic-looking numbers. Matching format is not proof.

How is this different from a fake Amazon customer service call?

Holding-fee scams center on a delivery surcharge link. Fake Amazon CS calls impersonate account support with unauthorized charges, refunds, codes, or remote access.

Is a $1.99 fee too small to be a scam?

Small amounts are intentional-they train you to type card data. The card theft is the goal.

What if I only entered an address?

Still risky. Watch for follow-up phishing that references that package story.

Do I need paid antivirus to avoid a holding-fee scam?

No. Ignoring cold links and checking tracking yourself is enough. Buy-nothing is valid.

If you still want a paid suite

Avoiding a package holding fee delivery 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

* Phishing Scams (FTC)
* ReportFraud.ftc.gov
* IdentityTheft.gov
* USPS.com

Also read

* How to spot a fake delivery text scam
* How to spot a fake Amazon customer service call
* How to spot a phishing email
* How to spot a gift card scam
* How to report a scam to the FTC