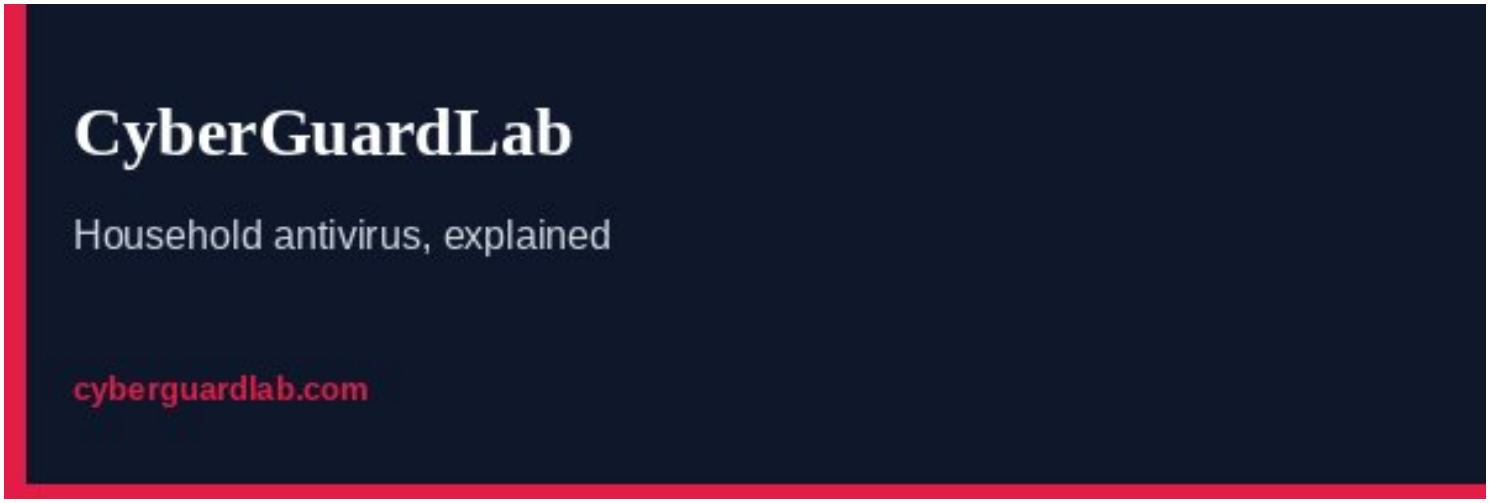
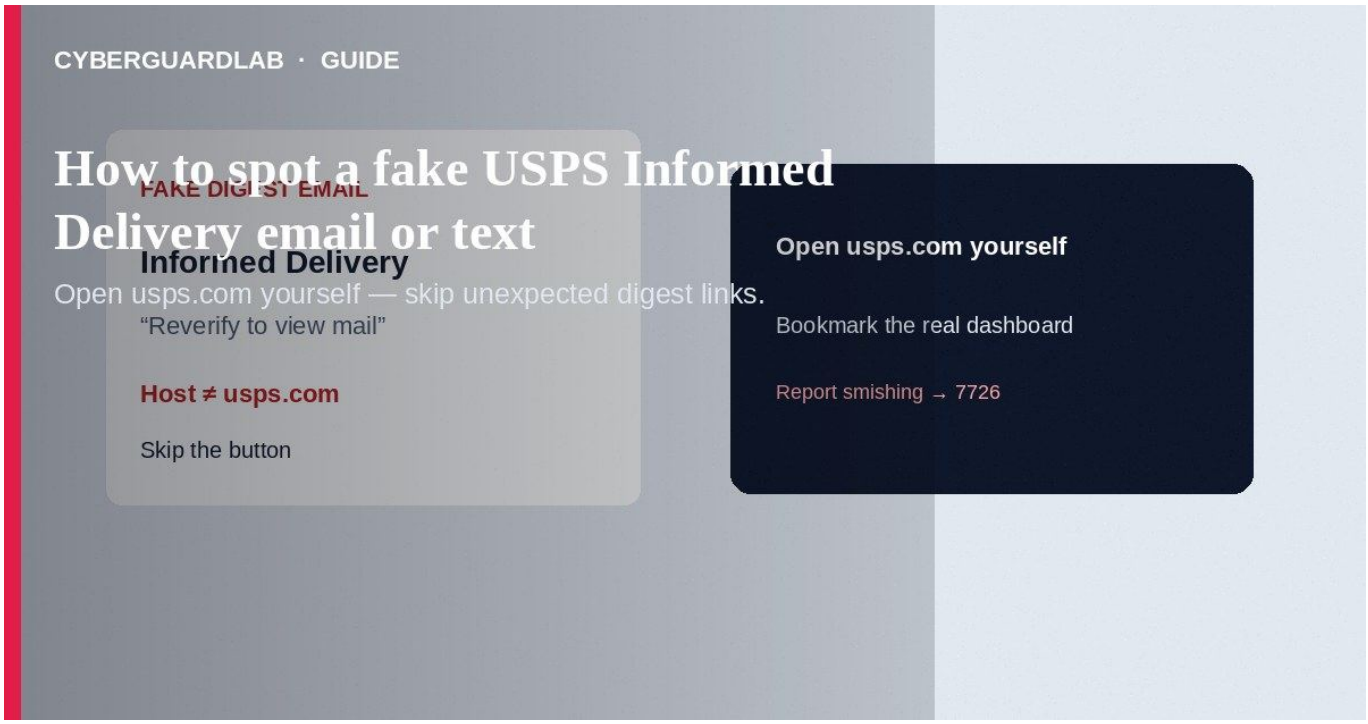


How to spot a fake USPS Informed Delivery email or text

https://cyberguardlab.com/blog/usps-informed-delivery-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 USPS Informed Delivery email or text pretends your mail preview, package, or USPS.com account needs "verification," then pushes a look-alike login or fee page. Real Informed Delivery is free and lives on USPS.com. Do not use unexpected links-open Informed Delivery yourself from a bookmark or by typing usps.com. This guide is Informed Delivery / USPS login phishing-not general fake delivery texts alone, and not bank-account first-hour recovery.

What this scam looks like

Subject or SMS lines include "Your Informed Delivery digest is ready-view mail," "Package held-confirm address," "USPS account locked-reverify," or "Pay a small fee to release your package." The branding looks like USPS, but the link host is not usps.com or email.informeddelivery.usps.com. Some pages ask for USPS.com passwords, card numbers, SSN digits, or a "redelivery fee."

Related cues overlap how to spot a phishing email. Smishing texts with strange tracking links follow the same rule: open USPS.com yourself.

Legitimate vs scam cues

Cue | Likely legitimate | Likely scam

You started it | You enrolled at USPS.com / Informed Delivery settings | Cold "sign up now" or "reverify" link you did not request

Link target | usps.com or Informed Delivery dashboard you opened yourself | Look-alike host, shortened URL, or unexpected redirect

Fees | Informed Delivery itself is free | "Release fee," gift-card payment, crypto, or wire

Package tracking texts | You started tracking with a real tracking number | Unsolicited text with a link; USPIS: USPS does not send tracking texts with links you did not request

Login ask | You typed usps.com yourself | Email/SMS button demands password, SSN, or card to "view mail"

What to do if you get one

* Do not click the Informed Delivery or "track package" button in the message. Do not open attachments.
* Open a browser yourself and go to USPS Informed Delivery or usps.com-not the message's URL.
* If you use Informed Delivery, turn on multifactor authentication in your USPS.com account settings when offered.
* Expecting a real package? Track it on USPS.com with the number from the seller or carrier email you already trust-not from the suspicious text.
* Report USPS-related smishing to the U.S. Postal Inspection Service (spam@uspis.gov) and forward scam texts to 7726. Report phishing at ReportFraud.ftc.gov.
* If you typed a USPS.com password on a fake page: change it on the real usps.com site from a clean device; enable MFA;

change any reused passwords.
* If you entered a card or bank details: call the bank/issuer, freeze or replace the card, watch statements, and use IdentityTheft.gov if identity data was exposed.
* Scan the device with Norton or Bitdefender; one primary product is enough (TotalAV, McAfee, or Avast). Microsoft Defender plus careful habits remains a valid "buy nothing" path.

Extra caution on "pay a fee to release your package"

USPS package tools you start yourself do not require gift cards, crypto, or surprise "release" fees via a text link. Hang up on callers who demand payment while a fake tracking page is open. Real carrier help starts from usps.com contact paths you open yourself.

FAQ

I already use Informed Delivery-how do I open the real digest?

Prefer the dashboard or app after you navigate to USPS.com yourself. When unsure about an email button, ignore it and open the service from a bookmark.

USPIS says tracking texts with links are scam-what about Informed Delivery emails?

Treat unexpected "click to view mail / reverify" links the same way: open the real site yourself. Do not trust the message's host.

The message shows a grayscale mail image-is it real?

Not necessarily. Branding and sample images are easy to copy. Domain and whether you opened usps.com matter more.

Will MFA stop this?

MFA on your real USPS.com account helps after credential theft. It does not make a fake login page safe-never type secrets on a page you reached from a cold link.

How is this different from a generic fake delivery text?

Informed Delivery phishing specifically targets USPS.com / mail-preview accounts so thieves can watch your mail or redirect packages. Same rule: no unexpected links.

If you still want a paid suite

Spotting Informed Delivery phishing does not require paid antivirus. Open official sites yourself and buy nothing if Defender habits are solid. If you want multi-device paid protection, use only these on-site paid links: Norton (paid link), Bitdefender (paid link), TotalAV (paid link), McAfee (paid link), Avast (paid link).

Sources

* USPS: Informed Delivery overview
* USPIS: Smishing - package tracking text scams
* FTC: How to recognize and avoid phishing scams
* CISA: Recognize and report phishing
* FTC: ReportFraud.ftc.gov

Also read

* How to spot a fake delivery or package text scam
* How to spot a phishing email
* Credit card fraud: first hour
* Clicked a phishing link: first hour
* How to report a scam to the FTC
* Is Microsoft Defender enough?