

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a fake FedEx delivery text

Read online: <https://cyberguardlab.com/blog/fake-fedex-delivery-text>

Published October 2, 2026 | Updated October 2, 2026

Short answer

Ignore the track / reschedule / pay-fee link in an unexpected FedEx delivery text; verify only at fedex.com or the FedEx app you open yourself; never pay a "delivery fee" or enter card details from a cold message.

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 FedEx delivery text

Ignore the fee link. Track your package yourself in the FedEx app or site



A fake FedEx delivery text (or email) is an unexpected SMS, iMessage, or message that claims your FedEx package has a "delivery exception," needs a "reschedule," is stuck in "customs," or requires a "fee" / "track package" tap through a cold link. Real FedEx tracking and delivery controls live inside the FedEx experience you open yourself - fedex.com tracking, the FedEx app you installed, or FedEx customer support you look up yourself - not inside a cold shortener from an unexpected

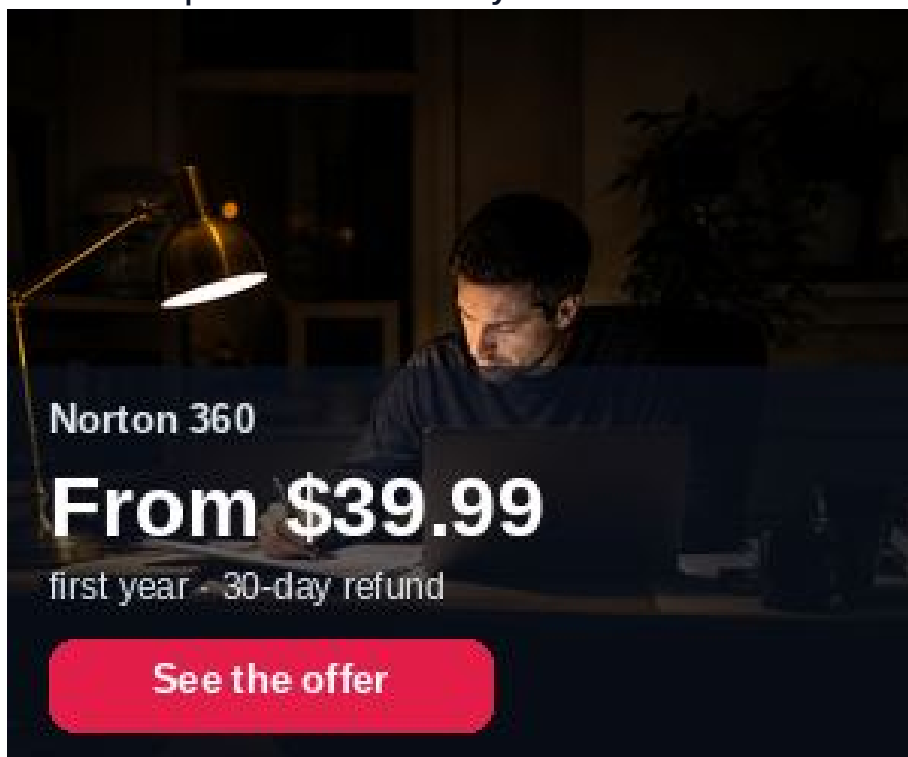
text. FedEx publishes tracking and customer-support pages; the safe habit is to ignore the cold link, track only after you open FedEx yourself, and never pay a "delivery fee" from a text. This page is about FedEx-branded delivery exception / reschedule / customs / pay-fee / track-package phishing only. The generic multi-carrier cousin is Fake delivery text scam. Related first-hour steps: Clicked a phishing link - first hour. CyberGuardLab is independent. Referral fees may affect product placement on other pages. Buying nothing and sticking to free verification habits is a valid outcome.

The short answer

Ignore the track / reschedule / pay-fee link in an unexpected FedEx delivery text; verify only at fedex.com or the FedEx app you open yourself; never pay a "delivery fee" or enter card details from a cold message.

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](https://cyberguardlab.com/norton)

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

What a fake FedEx delivery text usually looks like

Scammers copy FedEx delivery language: "delivery exception," "unable to deliver," "reschedule your package," "customs fee due," "holding fee," or "track your shipment." The job is credential theft, card theft, malware, or a small "fee" cash-out.

Common shapes US households report:

- * SMS or iMessage claiming FedEx could not deliver with a short link to "reschedule," "update address," or "confirm delivery."
- * Email about a FedEx "delivery exception" or "customs clearance fee" with a bright Track / Pay / Update button that does not land on fedex.com.
- * Look-alike FedEx tracking page after you tap - then a card / address / "fee" harvest, or a password on a fake login.
- * "Pay a small fee to release your package" pitch that mixes a real-looking tracking number with a payment form outside FedEx.
- * Follow-up after any reply or tap - once you engage, expect more "courier" texts or a scripted call. Related multi-carrier lure: Fake delivery text scam. Related first-hour steps: Clicked a phishing link - first hour.

FTC phishing and spam-text guidance: do not click links in unexpected messages; if you think it might be real, contact the company with a website or phone number you know is real; forward scam texts to 7726 (SPAM) and report at ReportFraud.ftc.gov.

We do not claim FedEx "never texts or emails about deliveries." FedEx may send real shipment notices. The safe habit is always the same: leave the unexpected message, open fedex.com or the FedEx app yourself, and manage tracking only inside a session or channel you started.

Fake FedEx delivery text vs real FedEx notice vs generic delivery-text scam

Signal | Fake FedEx delivery / exception / fee message | Real FedEx notice (typical) | Related lure (generic delivery text)

Opening hook | "FedEx delivery exception - reschedule / customs / pay fee / track now." | Shipment updates you can also see after you open FedEx tracking yourself. | "Your package from [carrier] needs action - tap to track."

Ask | Cold link, card "to release package," password on a look-alike page. | Usually none inside the message - track inside FedEx you open yourself. | Cold multi-carrier track / fee link (see Fake delivery text scam).

Pressure | Same-day return to sender, "fee doubles tomorrow," customs countdown. | Normal delivery calendar; you verify on your schedule. | Same-day loss of package or fee countdown across brands.

Safe next step | Ignore link. Type fedex.com or open the FedEx app yourself. | Confirm status only inside FedEx channels you start. | See Fake delivery text scam guide.

Related guide | This page | fedex.com tracking typed by you | FedEx app / customer support | Fake delivery text scam

If the page after the tap asks for a card, "delivery fee," or FedEx login on a domain that is not FedEx, stop - that is theft dressed as a package notice.

How to verify a FedEx delivery message (US household steps)

Do this when any unexpected FedEx exception / reschedule / customs / pay-fee / track message appears. You do not need a paid product to finish these steps.

* Do not tap the link, reply YES/NO, or call a number that lives only inside the message. Close the email or text. Do not discuss the "package" with a caller who contacted you first.

* Open FedEx the way you already trust. Type fedex.com yourself (or open FedEx tracking / the FedEx mobile app you installed earlier), use a bookmark you saved, or contact FedEx customer support through a path you look up yourself - not the track / pay / reschedule link from the unexpected message.

* Check shipment status only inside a session or channel you started. Look up the tracking number (if you already have one from a real retailer or sender) on FedEx tracking you opened yourself. If nothing unexpected appears - or you were not expecting a FedEx package - treat the message as spam.

* Never pay a "delivery fee," "customs fee," or "holding fee" from a cold text, and never enter card or FedEx login details on a page that arrived from that message. Legitimate FedEx tracking does not require you to trust an unexpected shortener or look-alike domain. International shipments can owe real duties or taxes; if you are expecting one, open fedex.com or the FedEx app yourself, look up the tracking number, and pay any real charge only from there.

* If you already tapped, typed a password, or entered a card, treat the first hour as incident response. Change passwords from sessions you started if you typed any; call the number on the back of your card to watch for fraud. Follow Clicked a phishing link - first hour. Report at ReportFraud.ftc.gov; if identity data was stolen, use IdentityTheft.gov.

* Report the message and tell the household. Mark the email as phishing / junk; forward scam texts to 7726 (SPAM); file at ReportFraud.ftc.gov. Agree that nobody tracks FedEx, reschedules, or pays a delivery fee from unexpected links - only via fedex.com or the FedEx app you open yourself. Checklist: How to report a scam to the FTC.

Signs the message is fake or unsafe (scan table)

Use this as a quick pass before you spend money or time.

Sign | Why it matters | What to do

Track / reschedule / pay / customs link lives only inside the unexpected message | Card and credential theft | Ignore; open

fedex.com or FedEx app yourself

URL is a shortener, misspelled FedEx name, or random form host | Phishing page | Never tap; type fedex.com

Urgent "return to sender in 2 hours" or "fee doubles today" | Fear used to skip verification | Slow down; check tracking inside FedEx you start

Asks for a "delivery," "customs," or "holding" fee by card / gift card / crypto | Direct cash-out | Stop; never pay from a cold text

You were not expecting a FedEx package, or tracking does not match a real order | Cold lure with fake tracking chrome | Ignore; confirm any real orders with the seller you bought from

You already replied, tapped, or spoke to a "courier agent" | Follow-up spam, malware, or payment fraud risk | Stop engaging; verify on fedex.com; run first-hour steps if you entered secrets

Free habits that reduce the blast radius

You do not need a new subscription to lower damage if a fake FedEx delivery text gets through.

- * Bookmark fedex.com tracking / the FedEx app; track only there - never from a cold delivery link.
- * Household rule: never use track / reschedule / pay-fee links inside unexpected FedEx emails or texts.
- * Differentiate brand costumes: USPS-branded Informed Delivery phishing is covered in USPS Informed Delivery scam; "pay to release a held package" across carriers is covered in Package holding fee scam.
- * Forward obvious scam texts to 7726; enable carrier and mailbox spam filtering when available.
- * Optional antivirus / web filtering is a separate layer after a bad tap; it does not replace the verify-on-fedex.com habit. Built-in Microsoft Defender plus those habits is enough for many households.

What this page is not

This page is not a guide to filing a real FedEx claim, not a review of FedEx shipping products, and not legal advice about a specific lost package.

It does not claim CyberGuardLab lab scores or "#1 anti-phishing" ranks. It does not tell you to ignore a real delivery change you can also see inside FedEx tracking you open yourself - it tells you to verify there, not in the cold message. It is not the generic multi-carrier delivery-text guide; for that costume, read Fake delivery text scam. It is also not the USPS Informed Delivery guide or the package holding-fee guide - those live at USPS Informed Delivery scam and Package holding fee scam. Official recovery and reporting stay with FedEx customer support, your card issuer, ReportFraud.ftc.gov, and IdentityTheft.gov if personal data was stolen.

If you decide a paid extra is a real job

Most households can handle fake FedEx delivery texts with the free steps above. Open a paid page only if you already named a job - for example broader web filtering, cross-device AV, or identity alerts after you gave a scammer personal data - and you will actually use it.

- * PC / Mac suite with phishing and web protections many households already compare: Norton plans (paid link; confirm renewal price).
 - * Independent-test-oriented suite option: Bitdefender plans (paid link).
 - * Household suite shopping starting point: TotalAV plans (paid link; confirm renewal).
 - * Multi-device bill under one vendor: McAfee plans (paid link; confirm device limit).
 - * Another suite path some homes already use: Avast plans (paid link).
- Buying nothing beyond free official-site / app verification habits is still valid. Paid links above are on-site only.

FAQ

Does FedEx really text or email about deliveries?

FedEx may send real shipment and delivery notices. That is why the safe test is not "FedEx never messages," but "I only track or reschedule inside fedex.com or the FedEx app I open myself - never from a cold link, and I never pay a delivery fee

from a text."

The message shows a tracking number and my city. Is that enough?

No. Tracking-like strings and city labels are easy to reuse from breaches, prior purchases, or guesswork. Trust the FedEx session or app you start yourself, not the message chrome.

I already entered a card or password on the "track / pay fee" page. What should I do first?

Call the number on the back of your card about possible fraud, then follow Credit card fraud - first hour. Change any password you typed from a site you open. Follow Clicked a phishing link - first hour. Report at ReportFraud.ftc.gov.

How is this different from a generic fake delivery text scam?

This page is FedEx-branded delivery exception / reschedule / customs / pay-fee phishing only. Fake delivery text scam covers the multi-carrier "your package needs action" costume. Same habit (ignore cold track/pay links; open the real carrier yourself), different brand focus. For USPS Informed Delivery branding or holding-fee pitches, see those dedicated guides.

How do I report a fake FedEx delivery text?

Mark the email as phishing / junk, forward scam texts to 7726 (SPAM), and file at ReportFraud.ftc.gov. Steps for the FTC side are in How to report a scam to the FTC.

Do I need paid antivirus to spot these messages?

No. Spotting is a verification habit: ignore the link, open fedex.com or the FedEx app, never pay a fee or enter secrets on a cold page. Microsoft Defender plus those habits is enough for many households. Antivirus can be a separate optional layer for malware after a bad tap; it does not replace that habit.

Sources

- * FedEx Tracking
- * FedEx Customer Support
- * Contact FedEx
- * FedEx Online tools
- * How To Recognize and Avoid Phishing Scams (FTC)
- * How to Recognize and Report Spam Text Messages (FTC)
- * ReportFraud.ftc.gov
- * IdentityTheft.gov
- * Avoiding Social Engineering and Phishing Attacks (CISA)

Also read

- * Fake delivery text scam
- * USPS Informed Delivery scam
- * Package holding fee scam
- * Clicked a phishing link: the first hour
- * How to report a scam to the FTC