

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a fake PayPal purchase alert

[Read online: https://cyberguardlab.com/blog/fake-paypal-purchase-alert](https://cyberguardlab.com/blog/fake-paypal-purchase-alert)

Published September 28, 2026 | Updated September 28, 2026

Short answer

Ignore the cancel / dispute link in an unexpected "PayPal purchase" or "unauthorized payment" message; verify only at paypal.com or the official PayPal app you open yourself; never enter your PayPal password or one-time code on a cold page.

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 PayPal purchase alert

Ignore the cancel link. Open PayPal yourself; never enter your password or code there



A fake PayPal purchase alert is an unexpected email, SMS, or push-style message that claims you just bought something you did not order, that a large payment "went through," or that you must "cancel," "dispute," or "confirm" through a link. Real PayPal activity lives inside the account you open yourself at paypal.com or the official PayPal app - not inside a cold cancel

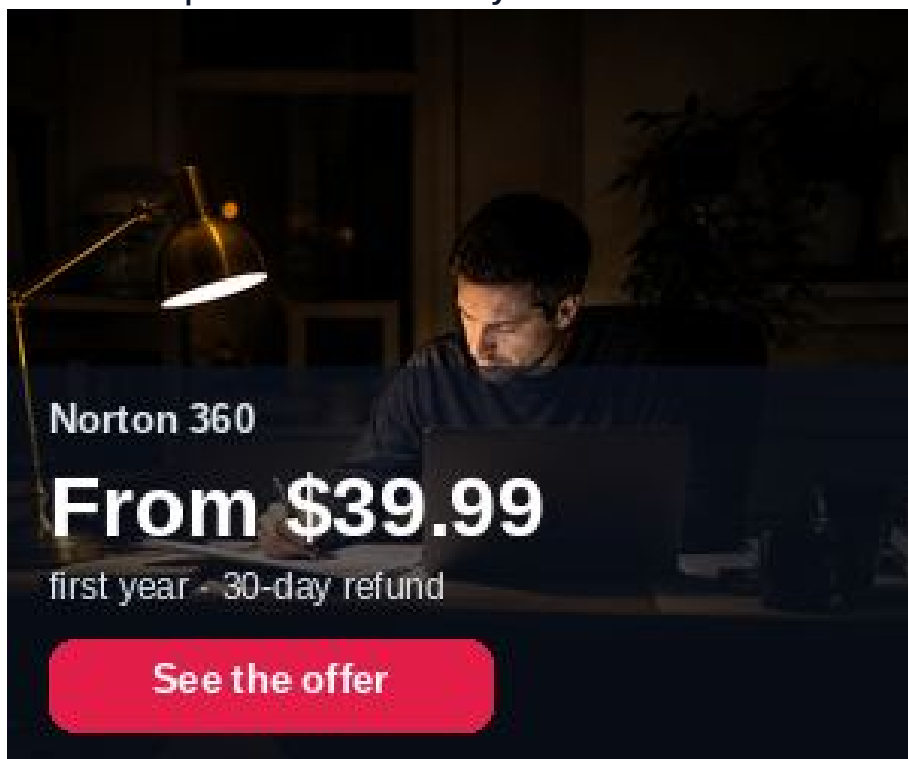
/ dispute button. PayPal's own phishing guidance warns that look-alike messages try to steal passwords, one-time codes, and bank or card details. This lure is related to other payment-app traps such as a Venmo payment request scam or a Zelle / Cash App payment scam. CyberGuardLab is independent. Referral 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 cancel / dispute link in an unexpected "PayPal purchase" or "unauthorized payment" message; verify only at paypal.com or the official PayPal app you open yourself; never enter your PayPal password or one-time code on a cold page.

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](https://trysecurities.com/offer/norton?dtm=gg&cid=)

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

What a fake PayPal purchase alert usually looks like

Scammers copy PayPal receipt language: "You sent \$489.99 to ...," "Unauthorized purchase - cancel now," "Payment on hold - confirm identity," or "Your account will be limited in 24 hours." The job is credential theft, card theft, or tricking you into sending money to "fix" a fake charge.

Common shapes US households report:

- * Email claiming a purchase you do not recognize with a bright "Cancel transaction" or "Dispute payment" button that does not land on paypal.com.
- * SMS or iMessage about an "unauthorized PayPal payment" with a short link to "stop the charge" or "secure your account."
- * Look-alike PayPal login page after you tap - then email, password, and often a one-time code harvest.
- * Fake invoice / seller dispute / limited-account notice that mixes real-looking case IDs with a cold "resolve now" link outside PayPal.
- * Follow-up after any reply or tap - once you engage, expect more "PayPal support" emails or a scripted call. Related payment-app angles: Venmo payment request scam | Zelle / Cash App payment scam.

FTC phishing 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; report at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov).

We do not claim PayPal "never emails about purchases." PayPal may send real receipts and security notices. The safe habit is always the same: leave the unexpected message, open paypal.com or the official app yourself, and manage activity only inside a session you started.

Fake PayPal purchase alert vs real PayPal notice vs related payment scams

Signal | Fake PayPal purchase / cancel message | Real PayPal activity notice (typical) | Related Venmo / Zelle / Cash App scam

Opening hook | "You paid \$X - cancel now / unauthorized purchase - dispute today." | Receipt or security details you can also see after you sign into PayPal yourself. | Unexpected payment request, "send back" refund trick, or cold "support" on another app.

Ask | Cold link, PayPal password, OTP, card, or a "refund fee" payment. | Usually none inside the message - manage Activity and Security inside signed-in PayPal. | Send money, gift cards, or remote access to "fix" a fake request.

Pressure | Same-day limit, "final chance to cancel," refund countdown. | Normal Activity timeline; you verify on your schedule. | Immediate "friend needs money" or "agent on the line" urgency.

Safe next step | Ignore link. Type paypal.com or open the official app. | Confirm Activity, login history, and linked banks only inside PayPal. | See Venmo and Zelle/Cash App guides; never send money to reverse a cold request.

Related guide | This page | paypal.com typed by you / official PayPal app | Venmo payment request scam | Zelle / Cash App
If the page after the tap asks for your PayPal password plus a one-time code or card on the same cold form, stop - that is credential theft dressed as a purchase alert.

How to verify a PayPal purchase alert (US household steps)

Do this when any unexpected PayPal purchase / cancel / dispute / limited-account 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 "purchase" with a caller who contacted you first.
- * Open PayPal the way you already trust. Type paypal.com yourself, use a bookmark you saved earlier, or open the official PayPal app already on your phone - not the cancel / dispute link.
- * Check Activity and Security only inside a signed-in session you started. Look at recent payments, login history, and linked banks or cards. If nothing unexpected appears, treat the message as spam.
- * Never enter your PayPal password, one-time code, or card on a page that arrived from a cold email or text. Legitimate PayPal account work does not require you to trust an unexpected shortener or look-alike domain. Do not send money to "cancel" or "refund" a charge you never made.
- * If you already tapped, typed a password or code, or entered a card, treat the first hour as incident response. Change your PayPal password from paypal.com or the official app you open; turn on 2FA if it was off; review linked banks and recent Activity; 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](https://reportfraud.ftc.gov); if identity data was stolen, use [IdentityTheft.gov](https://identitytheft.gov).
- * Report the message and tell the household. Mark the email as phishing / junk; forward scam texts to 7726 (SPAM); use PayPal's phishing-report options when available; file at [ReportFraud.ftc.gov](https://reportfraud.ftc.gov). Agree that nobody cancels PayPal purchases or "confirms identity" from unexpected links. 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

Cancel / dispute / confirm link lives only inside the unexpected message | Password and payment theft | Ignore; open paypal.com or the official app

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

Urgent "cancel in 15 minutes" or "account limited tonight" | Fear used to skip verification | Slow down; check Activity inside PayPal

Sender address is not a PayPal domain you recognize, or reply-to looks odd | Easy to spoof display names | Verify only inside a session you start

Page asks for PayPal password plus OTP / card on the same cold form | Credential + payment harvest | Stop; change password from official PayPal if you typed anything

You already replied, tapped, sent money, or spoke to a "PayPal agent" | Follow-up spam, malware, or account takeover risk | Stop engaging; verify on paypal.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 PayPal purchase alert gets through.

- * Bookmark paypal.com (or keep only the official app); manage Activity only there.
- * Household rule: never use cancel / dispute / confirm links inside unexpected PayPal emails or texts; never send money to "reverse" a cold alert.
- * Strong unique passwords + 2FA on email and PayPal limit what a stolen password can unlock.
- * 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-paypal.com habit.

What this page is not

This page is not a guide to filing a real PayPal Resolution Center dispute, not a review of PayPal fees, and not legal advice about a specific unauthorized charge.

It does not claim CyberGuardLab lab scores or "#1 anti-phishing" ranks. It does not tell you to ignore a real purchase you can also see inside your signed-in PayPal Activity - it tells you to verify there, not in the cold message. Official recovery and reporting stay with PayPal account security, your bank or 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 PayPal purchase alerts 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 verification habits is still valid. Paid links above are on-site only.

FAQ

Does PayPal really email or text about purchases?

PayPal may send real receipts and security notices. That is why the safe test is not "PayPal never messages," but "I only check Activity inside paypal.com or the official app I open myself."

The message shows my name or part of a transaction ID. Is that enough?

No. Names and transaction-like strings are easy to reuse from breaches, prior purchases, or guesswork. Trust the signed-in PayPal session you start yourself, not the message chrome.

I already entered my PayPal password on the cancel page. What should I do first?

Change your PayPal password from paypal.com or the official app you open. Turn on 2FA if it was off. Review Activity and linked banks. Follow Clicked a phishing link - first hour. Report at ReportFraud.ftc.gov.

How is this different from a Venmo or Zelle payment scam?

This page is about unexpected PayPal purchase / cancel links (email or text). The Venmo and Zelle / Cash App guides cover payment-request and "send money to reverse" tricks on those apps. Same money panic, different channel. Buyer or seller tricks that push you to pay outside PayPal's Goods and Services protection are covered in PayPal goods and services scam.

How do I report a fake PayPal purchase alert?

Mark the email as phishing / junk, forward scam texts to 7726 (SPAM), use PayPal's phishing-report options when available, 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 alerts?

No. Spotting is a verification habit: ignore the link, open paypal.com or the official app, never enter secrets on a cold page. Antivirus can be a separate optional layer for malware after a bad tap; it does not replace that habit.

Sources

- * What is phishing and how can I protect myself? (PayPal Help)
- * How do I report phishing or suspicious emails and phone calls? (PayPal Help)
- * Protect your PayPal account (PayPal Security)
- * 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

- * PayPal goods and services scam
- * Venmo payment request scam
- * Zelle / Cash App payment scam
- * Clicked a phishing link - first hour
- * How to report a scam to the FTC