

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a fake App Store receipt phishing email

<https://cyberguardlab.com/blog/fake-app-store-receipt-phishing>

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 App Store FAKE APP STORE receipt phishing email

Receipt / charge alert
Never tap Report a Problem in cold email.

Report a Problem → phish

Urgent 1-hour deadline

Don't tap the button

Settings → Media & Purchases

Type reportaproblem.apple.com

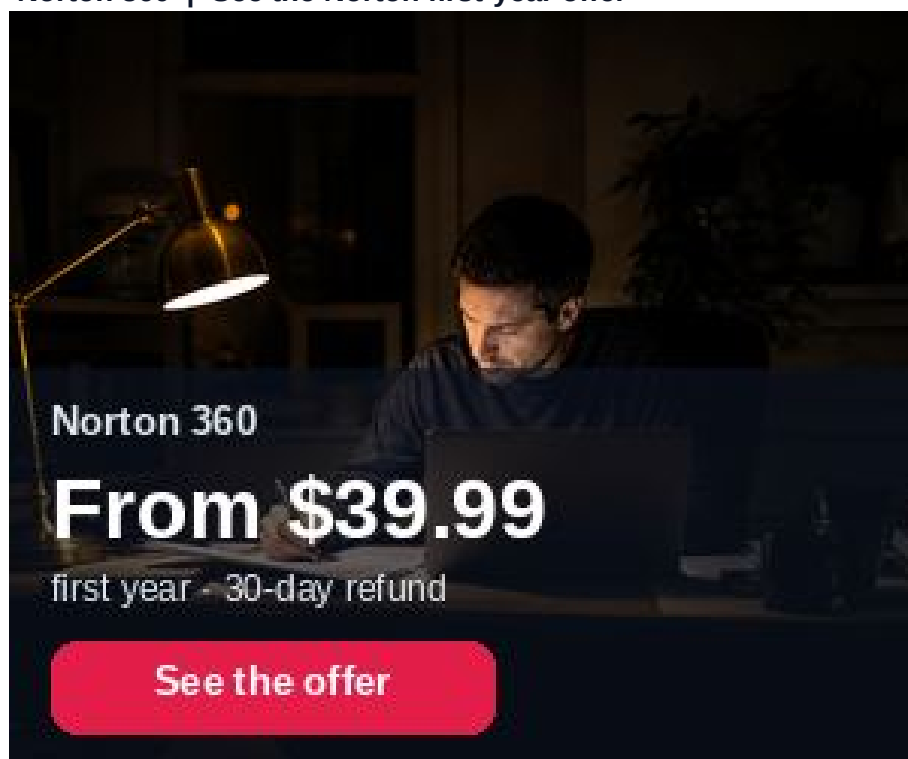
A fake App Store receipt phishing email claims you were charged for an app, subscription, or in-app purchase you do not recognize-then pushes a "Cancel," "Refund," or "Report unauthorized purchase" button that leads to an Apple ID password or card harvest page. Do not use the email's links. Check real purchases in Settings -> [Your Name] -> Subscriptions / Media & Purchases or report a problem through Apple's official purchase history tools you open yourself. This guide is about fake App Store receipts-not fake iCloud storage phishing, not configuration profiles, and not Google Play billing phishing.

1. What this scam looks like

Subjects like "Your receipt from Apple," "Unauthorized purchase of \$49.99," or "Subscription renewed." The logo looks right; the domain does not (apple-support-secure.com, appstore-billing.net, etc.). Some include a PDF "invoice." Urgency is the hook: cancel in 30 minutes or the charge becomes permanent. Real Apple purchase mail can exist-still verify inside the Settings app or reportaproblem.apple.com typed by you.

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>

Shared payment methods make surprise-receipt lures more convincing. Agree as a household that nobody taps refund links from email-everyone checks Subscriptions in Settings first.

2. Legitimate vs scam cues

Cue | Likely legitimate | Likely scam

How you review the charge | Settings / App Store purchase history / official Report a Problem | Button inside the email only

Sender domain | Apple domains you carefully verify | Look-alike hosts, free mail, odd TLDs

Ask | Informational receipt; you navigate yourself to manage | Immediate Apple ID password + full card on one page

Tone | Matter-of-fact purchase details | "Legal hold," "account suspended in 1 hour"

Attachment | Often none, or cautious handling | Odd HTML/PDF urging macros or login

3. What to do if you get the email

* Do not tap Cancel/Refund/Verify in the message.

* On iPhone: Settings -> [Your Name] -> Subscriptions and purchase/media settings to see real charges. Use Apple's Report a Problem flow from purchase history when needed.

* If the charge is real and unwanted, cancel the subscription in Settings and follow Apple's refund guidance-still without the phishing link.

* Report phishing in Mail when available; file at ReportFraud.ftc.gov for clear fraud attempts.

* Delete the message; warn family who share the Apple Account.

4. If you already typed your Apple ID password

* Change the Apple Account password on a trusted device; review devices and sign-out unknowns.

* Check payment methods; call your bank if card data was entered.

- * Review configuration profiles in case a "receipt helper" profile was offered.
- * Enable or confirm Stolen Device Protection and recovery contacts so a follow-on theft is harder.
- * Scan PCs that opened the link with Norton or Bitdefender; keep one primary suite (TotalAV, McAfee, Avast also listed on-site).

FAQ

Does Apple send App Store receipts by email?

Apple can send purchase confirmations. Treat every unexpected "unauthorized charge" email as hostile until Settings shows the same purchase.

How is this different from Google Play billing phishing?

Same pattern, different brands. Google Play fakes are covered in fake Google Play billing phishing-do not mix the official review paths.

The amount matches a game my kid plays.

Still open Settings yourself. Family Sharing purchases belong in Apple's UI, not a stranger's refund form.

Should I call the number in the receipt?

No. Use support.apple.com or the Apple Support app you launch yourself.

If you still want a paid suite

Avoiding how to spot a fake App Store receipt phishing email 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

- * Apple Support: Recognize and avoid phishing messages
- * Apple Support: View your purchase history
- * FTC: Phishing scams
- * FTC ReportFraud

Also read

- * How to spot a fake iCloud storage full phishing email
- * How to spot a fake Google Play billing phishing email
- * How to check for configuration profiles on iPhone
- * How to spot a phishing email
- * How to use Safari passkeys instead of passwords on iPhone