CyberGuardLab

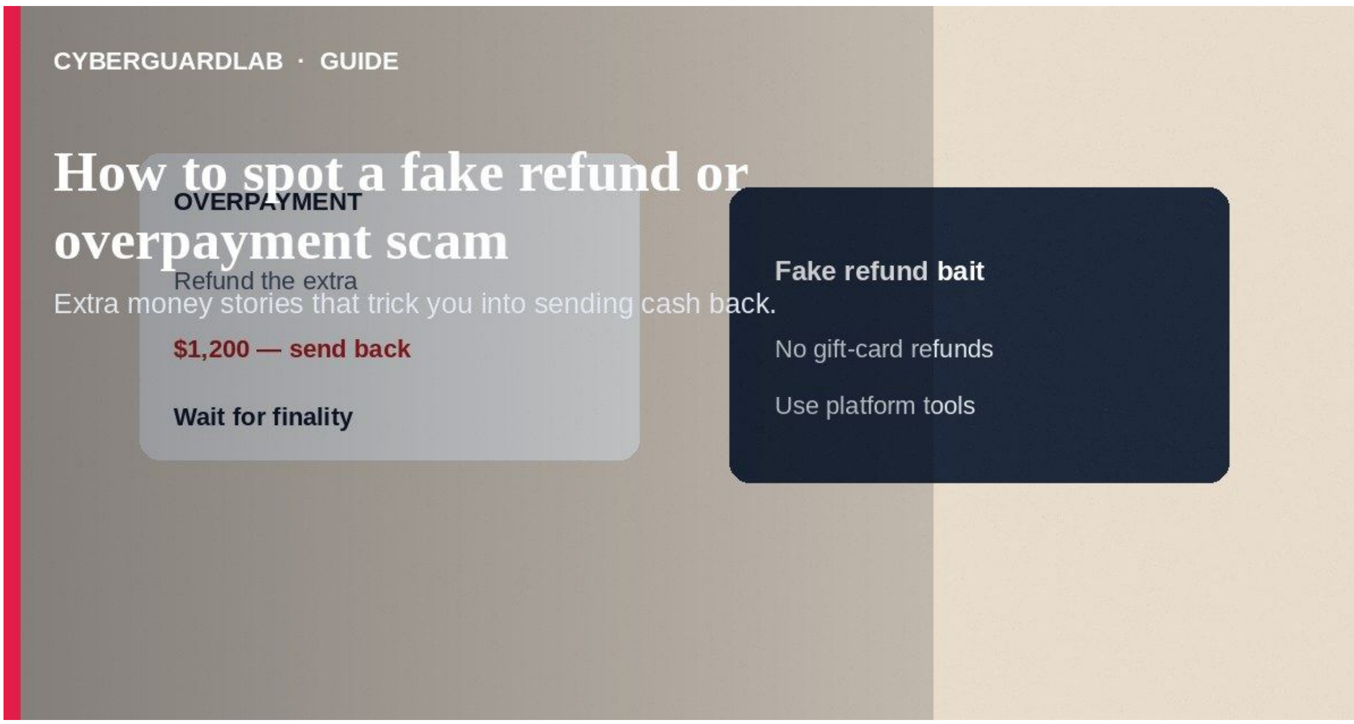
Household antivirus, explained

cyberguardlab.com

How to spot a fake refund or overpayment scam

https://cyberguardlab.com/blog/fake-refund-overpayment-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 refund or overpayment scam tells you that you were paid or credited too much-or that a refund is waiting-then tricks you into sending the "extra" back by wire, cash app, gift cards, or crypto before the original payment bounces. Do not return money from a check, transfer, or marketplace payment until your bank confirms it is real and final. Do not buy gift cards to "process a refund." If you already sent funds, stop contact, document everything, and report to the FTC.

This guide covers overpayment and fake-refund bait-not buy-now-pay-later account takeover where someone else opens BNPL credit in your name. Check-based versions overlap with the fake check scam. Cash-app versions overlap with Zelle and Cash App payment scams. No software purchase required.

1. How fake refund and overpayment scripts work

A buyer accidentally pays more than the price and asks you to refund the difference. A company says you overpaid a bill and will send a check-deposit it, then wire part back. A caller claims Amazon, your bank, or a store needs you to buy cards so they can push a refund.

* Marketplace overpay - Partial refund requests after a too-large payment.
* Fake-check wrap - Deposit a check, return the excess (fake check scam).
* Cold refund calls - Gift cards or crypto to release a refund.
* Job or rental twists - Same overpay-and-return script with a hiring or housing story.

2. Red flags before you send money back

Cue	Likely legitimate	Likely scam
Refund path	Credit returns to the original payment method automatically	You must send money somewhere to release a refund
Overpayment story	Rare; merchant adjusts the order themselves	Buyer urgently needs the difference returned today
Payment instrument	Known customer with a clear history	Unexpected check, money order, or third-party transfer
Pressure	Normal support timelines	Accounting closes in an hour-send now
Method of return	In-platform refund tools	Gift cards, crypto, wire, or Friends and Family
Who contacted you	You started a return in the store's official flow	Cold call/text promising a surprise refund

3. Safer habits (buy-nothing)

* Do not return extra money until your bank says the deposit is good and final-ask how long that takes.
* Refuse gift cards as a refund method.
* For marketplace sales, use the platform's refund tools only.
* Hang up on cold refund calls; open your bank or store app yourself.

* Be wary of job or rental offers that overpay on day one.
* Compare check-based scripts with fake check scam guidance.

4. If you already paid

* Stop sending any more remaining-balance payments.
* Contact your bank or payment app's fraud team immediately with transaction IDs (FTC if you were scammed).
* If a check was involved, ask the bank about return timelines and next steps.
* Save chats, envelopes, check images, and caller details.
* Report at ReportFraud.ftc.gov; use IdentityTheft.gov if account numbers were shared.
* If you installed remote software or visited a fake refund portal, change passwords and ignore recovery callers.

FAQ

The check cleared overnight. Is it safe to refund?

Not necessarily. Some checks appear to clear and are later reversed. Follow your bank's guidance on finality before sending money out.

A store said I need gift cards for a refund. Ever legitimate?

Treat that as fraud. Real refunds go back to the original payment method.

How is this different from BNPL account takeover?

Overpayment/refund scams trick you into sending money you think is extra. BNPL takeover is someone else using your identity or login to open or abuse buy-now-pay-later credit.

What if the overpayment came through PayPal?

Still high risk if someone asks for a partial return outside normal dispute tools. Verify carefully and prefer platform processes.

Can I keep the overpayment if I never send it back?

If funds are stolen or reversed, you may still owe your bank. Do not spend unexpected windfalls.

Do I need paid antivirus to avoid a refund overpayment scam?

No. Waiting for payment finality and refusing gift-card refunds is enough. Buy-nothing is valid.

If you still want a paid suite

Avoiding a fake refund or overpayment 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

* Fake Check Scams (FTC)
* ReportFraud.ftc.gov
* IdentityTheft.gov
* Imposter Scams (FTC)

Also read

* How to spot a fake check scam
* How to spot a buy-now-pay-later account takeover
* How to spot a Zelle or Cash App payment scam
* How to spot a Cash App refund or deposit scam
* How to report a scam to the FTC