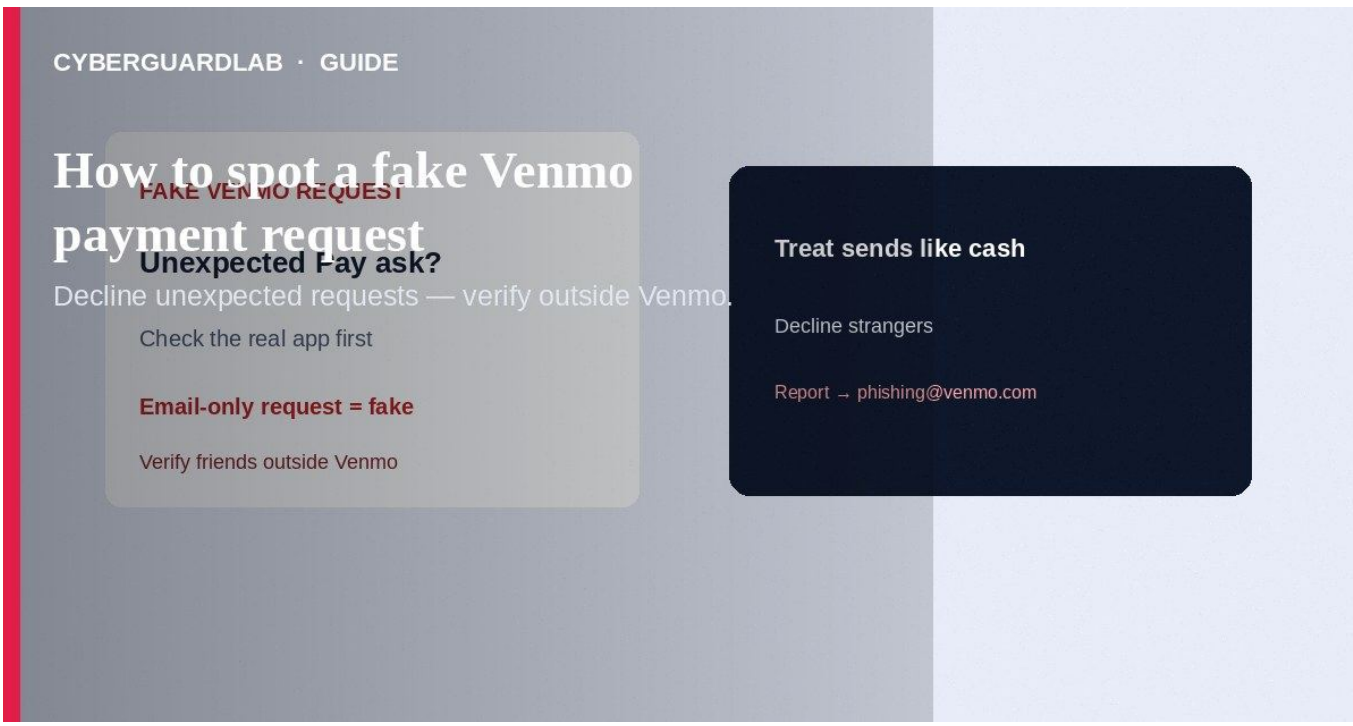
CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a fake Venmo payment request

https://cyberguardlab.com/blog/venmo-payment-request-scam



A fake Venmo payment request is when someone asks you to send money through Venmo-or sends a look-alike email/text about a request-so you pay a scammer instead of a real person. Venmo Help says unexpected requests from strangers should be declined, and a request that "looks like" a friend or relative should be confirmed outside Venmo before you act. The FTC treats payment-app sends like cash: once money leaves, it is hard to reverse. This guide focuses on Venmo payment request scams (in-app requests, fake request emails, urgency to pay). It is not a Zelle/Cash App overview and not a PayPal Goods and Services dispute guide.

How a fake Venmo request usually works

* Stranger request - Anyone can send a Venmo request. If you are not expecting one, decline it.
* Impersonated friend/relative - A request appears to come from someone you know (hacked account, look-alike username, or spoofed notice). Venmo recommends contacting that person on a channel you already trust outside Venmo before

paying.
* Email/text "you have a request" that is not in the app - Venmo Help: if an email says you have a payment request but that request does not appear in the Venmo app or on the web, treat it as a fraudulent email.
* Prize / fee / "send to unlock" - FTC: scammers may claim you won something or must pay a fee through a payment app.
* Urgent "account problem" push - Phishing emails/texts pretend to be Venmo and push you to click, enter credentials, or pay. Venmo Help: do not click links; open the official app yourself.

Red flags before you tap Pay

Cue | Safer habit | Scam signal

Who is requesting | Someone you know and can verify out-of-band | Stranger, look-alike @username, or "friend" you cannot reach elsewhere

Where the notice lives | Request visible in the real Venmo app/web | Email/SMS about a request that never shows in-app

What they ask | Clear split of a shared bill among people you know | Prize fee, "verification" payment, refund-to-send, or gift-card/crypto add-on

Pressure | You can wait and confirm | Act now, don't tell anyone, only pay via this request

Message style (fake Venmo mail) | You open Venmo yourself if unsure | Generic "Dear user," urgent account warnings, odd links/attachments

Steps: what to do when a Venmo request arrives

* Pause - Do not pay, click email/SMS links, or share one-time codes.
* Check the app - Open Venmo yourself (app icon or typed site). Confirm whether a real request appears. If only the email/SMS mentions it, treat that message as fake per Venmo Help.
* Decline strangers - Unexpected request from someone you do not know -> decline.

* Verify "friends" outside Venmo - Call or text a number you already have for that person. Do not use contact info only inside the suspicious thread.
* Never return a mystery payment yourself - Venmo Help: if a stranger pays you by mistake, do not try to return the money yourself-contact Venmo Support (and consider blocking them).
* Report phishing - Forward suspicious Venmo-looking email/SMS/website details to phishing@venmo.com as Venmo instructs (screenshot SMS including full number; do not put sensitive personal data in that automated inbox).
* If you already paid - In the Venmo app go Me -> Settings -> Get Help -> Chat With Us (or Venmo's contact options), ask to reverse/refund, then report at ReportFraud.ftc.gov. Change your Venmo password and review recent activity if you entered details on a fake site.

Safer Venmo habits (buy-nothing)

* Treat Venmo sends like handing over cash.
* Turn on multi-factor / PIN protections Venmo offers; use a unique password.
* Family rule: no emergency Venmo pays until a known-good callback confirms the story.
* Prefer a credit card at a real merchant checkout when a purchase is involved-cards often have stronger dispute paths than P2P cash-like sends (FTC payment-method guidance).
* Microsoft Defender (or your built-in OS protections) is enough for many households if the risk was a phishing page; judgment and declining fake requests are the main defense. Paid suites are optional.

FAQ

Is Venmo itself a scam?

No. Households use it every day. Scammers abuse requests, look-alike usernames, and phishing messages about requests.

Someone who looks like my cousin sent a Venmo request. What should I do?

Decline or ignore until you confirm with your cousin on a phone number or chat you already trust-outside Venmo. That is Venmo's own advice for friend/relative-looking requests.

I got an email about a Venmo request but nothing shows in the app. Is it real?

Venmo Help says that pattern can mean a fraudulent email. Do not click; open the app yourself and report phishing if needed.

Why is it hard to get Venmo money back?

The FTC compares many payment-app transfers to sending cash. Always ask Venmo to reverse it immediately, but do not assume a refund is guaranteed.

Do I need paid antivirus to avoid Venmo request scams?

No. Declining unexpected requests, verifying people out-of-band, and ignoring fake emails are enough. Buy-nothing is valid.

If you still want a paid suite

Spotting a fake Venmo request does not require paid antivirus. If you still want multi-device paid protection, use only these on-site links: Norton (paid link), Bitdefender (paid link), TotalAV (paid link), McAfee (paid link), Avast (paid link).

Extra caution

A polished Venmo logo in an email does not prove the message is real. Open the official app yourself, decline what you did not expect, and verify people outside the app.

Sources

* Venmo Help: Payment from a stranger / requests
* Venmo Help: Reporting fake or suspicious messages or emails
* FTC: Mobile payment apps - how to avoid a scam
* FTC: Do you use payment apps like Venmo, CashApp, or Zelle?

* FTC: What to do if you were scammed
* ReportFraud.ftc.gov

Also read

* Zelle and Cash App payment scams
* PayPal Goods and Services scams
* Cash App refund/deposit scam
* Is Microsoft Defender enough?
* Clicked a phishing link: first hour
* Fake password-reset email