

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a GoFundMe or crowdfunding donation scam

<https://cyberguardlab.com/blog/gofundme-crowdfunding-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.

CYBERGUARDLAB · GUIDE

How to spot a GoFundMe or crowdfunding donation scam

CROWDFUNDING CHECK

Who is the organizer?

Verify the organizer and photos before you give.

Reverse-search campaign photos

Gift cards / crypto = red flag

Money goes to the organizer

Confirm off-platform

Prefer known charities after disasters

Report fakes → [ReportFraud.ftc.gov](https://www.ftc.gov/identity-theft)

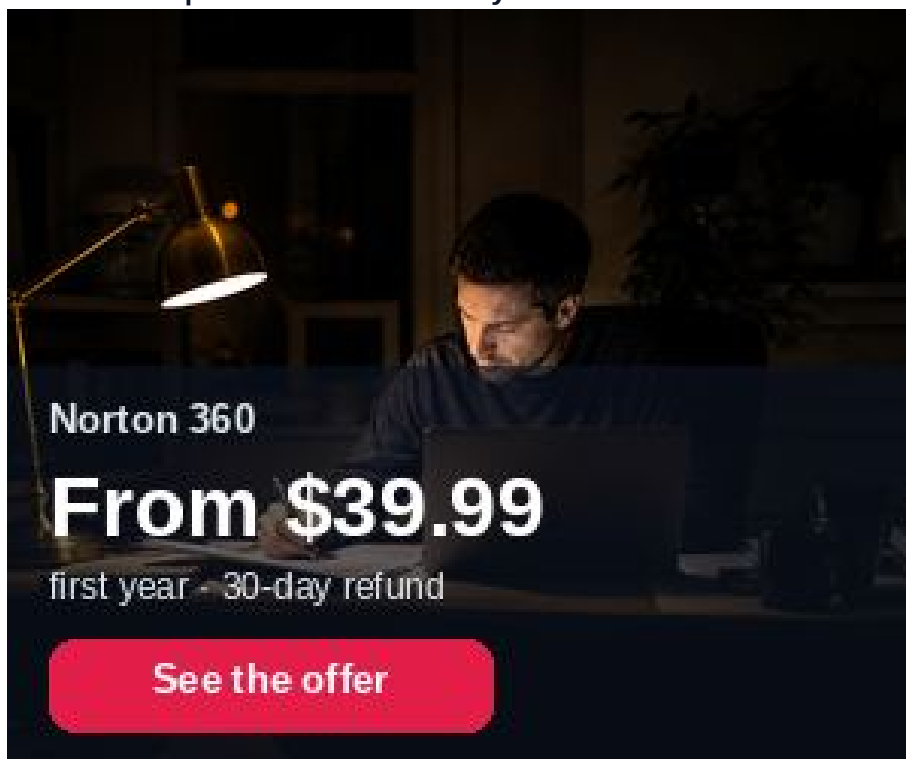
A GoFundMe or crowdfunding donation scam is a campaign (or share of one) that steals sympathy-and money-by faking a crisis, copying someone else's photos/story, or funneling funds to an organizer who never delivers to the claimed beneficiary. Money goes to the campaign organizer, not automatically to a verified charity. This guide is crowdfunding red flags and safer giving-not church collection plates, not crypto "recovery" firms, and not general charity phone-call rules alone.

How crowdfunding scams usually work

Platforms make campaigns easy to launch and fund quickly. Scammers exploit disasters, medical stories, and viral social shares. The FTC notes organizers control how money is spent and may keep fees or never pass funds along. The FBI's IC3 has warned that fake charities and crowdfunding accounts spike after mass-casualty and disaster events-pressure to "act fast" is a classic tell.

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>

Red flags vs safer checks

Check | Safer signal | Scam signal

Who organized it | Someone you know and can confirm off-platform | Stranger + urgent DM; friend only "liked" a post without knowing the organizer

Photos / story | Unique, consistent details | Reverse-image search finds the same photos on other campaigns or names

Payment ask | Normal card checkout on the real platform | Gift cards, wire, crypto, or off-platform "direct Venmo to help faster"

Charity claim | You can verify IRS tax-exempt status / state registration | Copycat charity name; vague "victims fund" with no details

Steps before you donate

- * Identify the organizer-not just the person pictured. Ask a friend who shared the link what they personally know.
- * Reverse-image search campaign photos. If they appear under other names or campaigns, walk away (FTC).
- * For disaster/tragedy giving, prefer charities you already know with a track record-ideally donate on the charity's own website.
- * Remember: donations to individuals are generally not tax deductible. If deductibility matters, use the IRS Tax Exempt Organization Search for a real charity.
- * Never pay with gift cards, wires, or crypto because a post "needs it now." Prefer credit card on a platform you navigated to carefully.
- * Read the platform's fee and payout rules so you know who actually receives funds.

If you already donated to a suspect campaign

- * Report the campaign to the crowdfunding platform (FTC lists reporting paths for major platforms including GoFundMe).
- * File at ReportFraud.ftc.gov.
- * For internet fraud tied to fake charities/crowdfunding after disasters, report to the FBI IC3 at ic3.gov.
- * Tell your state attorney general / charities regulator when a charity angle is involved.
- * Watch your statements for unexpected recurring charges; contact your card issuer about unauthorized charges.
- * Ignore anyone offering to "recover" your donation for an upfront fee-that's a second scam. Keep devices clean if you clicked odd links: Microsoft Defender is fine; optional on-site compares Norton, Bitdefender, TotalAV, McAfee, Avast.

Extra caution after disasters

Scammers move fastest in the first days after wildfires, storms, and mass-casualty events. Slow down, verify the organizer, reverse-search images, and when in doubt give through a known charity's official site instead of a stranger's campaign.

FAQ

A friend shared the GoFundMe-does that make it safe?

Not by itself. Contact your friend separately and ask what they know about the organizer and beneficiary before you give.

How is this different from a fake charity phone call?

Crowdfunding is person-to-person on a platform; charity-call scams often misuse look-alike nonprofit names. Both need independent research. See also charity donation scam.

Are medical crowdfunding campaigns automatically legitimate?

No. The FTC warns some medical crowdfunding promotes unproven treatments. Vet the organizer and claims independently.

Where do I report if I'm unsure which agency?

Start with the platform + ReportFraud.ftc.gov. For cyber-enabled fraud, add IC3. More on reporting: report a scam to the FTC.

Will antivirus detect a fake fundraiser?

No. Scam campaigns are social engineering. Antivirus only helps if a malicious link downloads malware.

If you still want a paid suite

Safer crowdfunding giving is research and payment hygiene-not a product purchase. Buy-nothing is valid. If you still want a paid suite, use only these on-site paid links: Norton ([paid link](#)), Bitdefender ([paid link](#)), TotalAV ([paid link](#)), McAfee ([paid link](#)), Avast ([paid link](#)).

Sources

- * FTC: Donating through crowdfunding and fundraising platforms
- * FTC: Before giving to a charity
- * FTC: ReportFraud.ftc.gov
- * FBI IC3 PSA: Beware of charitable fraud related to mass casualty and disaster events

Also read

- * How to spot a charity donation scam
- * How to report a scam to the FTC
- * How to spot a phishing email
- * Credit card fraud: first hour
- * How to spot an online romance scam
- * Is Microsoft Defender enough?