CyberGuardLab

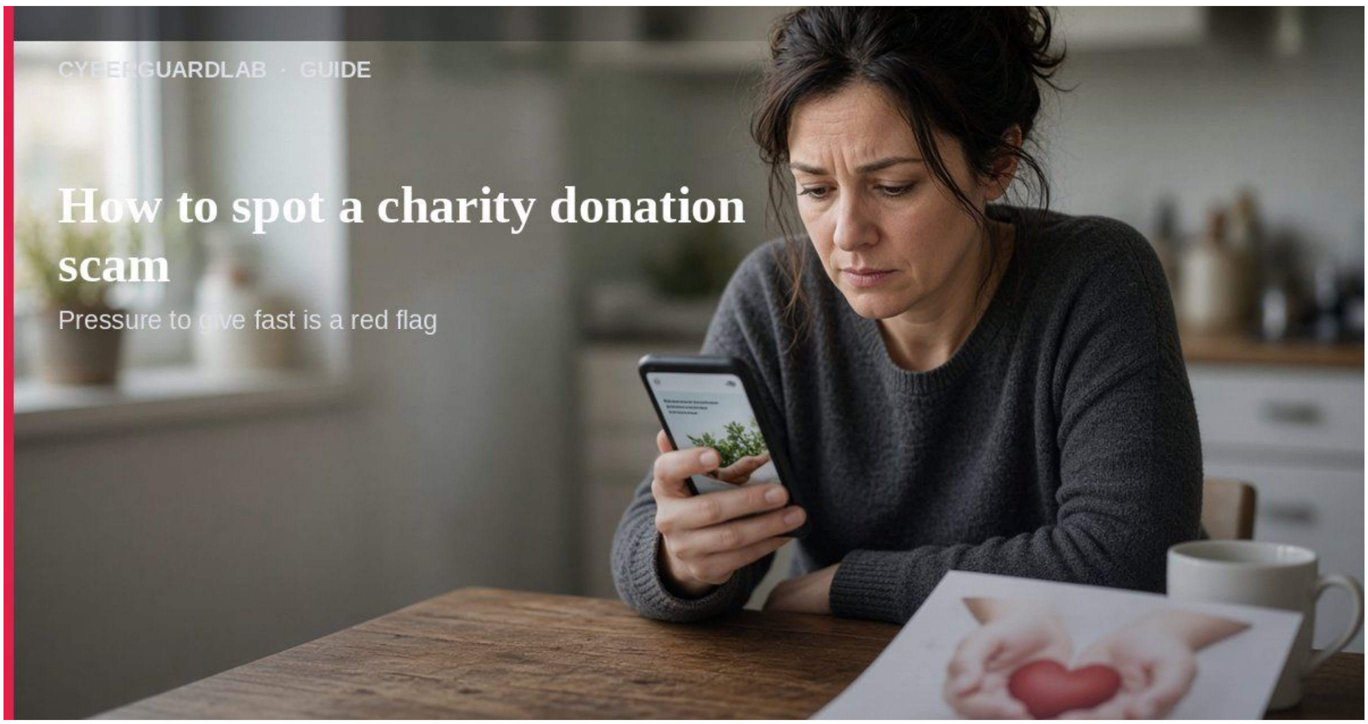
Household antivirus, explained

cyberguardlab.com

How to spot a charity donation scam

https://cyberguardlab.com/blog/charity-donation-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 charity donation scam is when someone pressures you to give money to a cause that is fake, misnamed, or mostly lining a fundraiser's pockets. Per the FTC's Before Giving to a Charity guidance, you should research the charity before you give, confirm the exact name and where the money goes, and treat high-pressure calls or social links with care. This guide is about donation and fundraising asks, not gift card payment scams, lottery "prizes", or phishing emails. You do not need to buy antivirus to pause and verify a charity.

1. How fake charity asks usually work

From FTC charity and crowdfunding guidance:

Paid link

Norton 360 | See the Norton first-year offer

* Name confusion - A fundraiser uses a name that sounds like a well-known charity.
* Urgency after disaster - After floods, tornadoes, or other tragedies, strangers push "donate now" before you can check.
* Phone pressure - Calls ask for card numbers, gift cards, wires, crypto, or payment-app sends on the spot.
* Social or crowdfunding shortcuts - A friend shares a link; you assume it is safe. FTC: don't assume hyperlinks are accurate just because someone posted them.
* Inflated "gifts-in-kind" - Dishonest groups can mark up donated goods to look more successful while cash goes to overhead.

2. Four things to do before you donate

FTC checklist, adapted for a US household:

* Check the charity's own website - Look for clear programs and how donations are used. If that detail is missing, be suspicious.
* Confirm registration - Most states require charities and their fundraisers to register with the state charity regulator.
* Confirm tax-exempt status if that matters to you - Use the IRS Search for tax exempt organizations tool. Donations to political PACs or to individuals are not tax deductible.
* Prefer the charity's official site - Faster and safer than random social links or unfamiliar crowdfunding pages.

3. Phone calls asking you to donate

If someone calls for a donation, FTC says ask:

* Exact name, website, and mailing address of the charity
* Whether the donation is tax deductible (then verify in the IRS tool)
* How much of the gift goes to programs vs. fundraising

Fundraisers also have rules: they must disclose who they are and why they are calling; they can't call before 8 a.m. or after 9 p.m.; they can't lie about the mission, tax deductibility, or how money is used; caller ID should show the charity or fundraiser. If they break those rules, find another way to give.

Ask to be put on the charity's do-not-call list if you want the calls to stop. Fundraising calls can still reach numbers on the

National Do Not Call Registry.

4. Crowdfunding and social donations

From FTC crowdfunding guidance:

* Safest gifts go to campaigns run by people you know and trust.
* Donations to individuals are not tax deductible, even if that person later gives to a charity.
* After disasters, stick to charities you already know, with a track record for relief work.
* Online platforms may take fees before money reaches the charity - if fee details are unclear, donate on the charity's own site instead.
* Report a crowdfunding scam to the platform first, and report problem local charities to your state regulator.

5. If you already sent money

* Contact your bank, card issuer, or payment provider as soon as you can.
* Follow FTC recovery steps for people who paid a scammer.
* Report at ReportFraud.ftc.gov with the fundraiser name, charity name, phone, website, address, and what you were told.
* Warn family so the same script doesn't hit them next.

FAQ

How do I spot a charity donation scam?

Pressure to pay now, a name that only sounds familiar, refusal to give clear program details, or payment by gift card / wire / crypto / payment app are classic FTC red flags.

Is a social media donation link safe because a friend shared it?

Not by itself. FTC: verify who's asking and who's getting the money; prefer the charity's own site.

Will my donation be tax deductible?

Only if the organization is listed as tax-exempt in the IRS search tool. Gifts to individuals or PACs are not.

Is Microsoft Defender required here?

No. This is a donation / social-engineering problem. Defender is optional later if you also clicked a shady link on a PC - see Is Microsoft Defender enough?.

Where do I report it?

ReportFraud.ftc.gov. USAGov also has a where to report a scam guide.

If you still want a paid suite

Stopping a fake charity ask does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is verifying the charity and refusing irreversible payment methods. If the household later wants multi-device paid protection, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* Before Giving to a Charity (FTC)
* Donating Through Crowdfunding and Fundraising Platforms (FTC)
* Donating to Charity topic hub (FTC)
* How To Avoid a Scam (FTC)
* Search for tax exempt organizations (IRS)
* ReportFraud.ftc.gov (FTC)
* Learn where to report a scam (USAGov)

Also read

* How to spot a gift card scam

* How to spot a lottery or prize scam
* How to spot a fake check scam
* How to stop spam text messages
* How to spot a phishing email