



National Indian Health Board NATIONAL TRIBAL COVID-19 RESPONSE

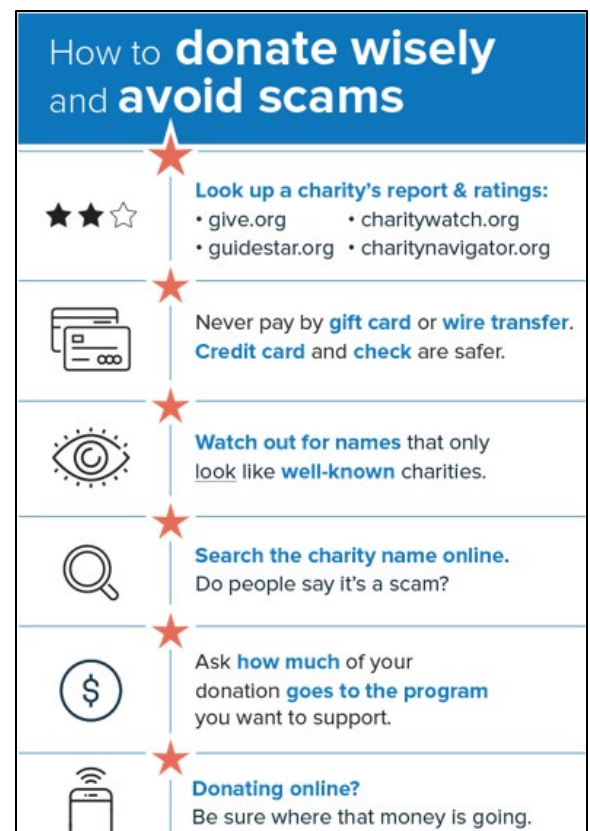
910 Pennsylvania Avenue, SE | Washington, D.C. 20003 | 202-507-4070 | www.nihb.org






Federal Agency Guidelines on Fraud during COVID-19

From the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA):

CISA TIPS

- Avoid clicking on links in unsolicited emails and be wary of email attachments.
- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. The Federal Trade Commission's page on Charity Scams has more information.
- Review CISA Insights on Risk Management for COVID-19 for more information.



How to donate wisely and avoid scams	
★★★	Look up a charity's report & ratings: • give.org • charitywatch.org • guidestar.org • charitynavigator.org
	Never pay by gift card or wire transfer . Credit card and check are safer.
	Watch out for names that only look like well-known charities.
	Search the charity name online. Do people say it's a scam?
	Ask how much of your donation goes to the program you want to support.
	Donating online? Be sure where that money is going.



National Indian Health Board NATIONAL TRIBAL COVID-19 RESPONSE

910 Pennsylvania Avenue, SE | Washington, D.C. 20003 | 202-507-4070 | www.nihb.org

From the Department of Health and Human Services:

HHS Tips

- Scammers are offering COVID-19 tests to Medicare beneficiaries in exchange for personal details, including Medicare information. **However, the services are unapproved and illegitimate.**
- Fraudsters are targeting beneficiaries in a number of ways, including telemarketing calls, social media platforms, and door-to-door visits.
- These scammers use the coronavirus pandemic to benefit themselves, and beneficiaries face potential harms. The personal information collected can be used to fraudulently bill Federal health care programs and commit medical identity theft. If Medicare or Medicaid denies the claim for an unapproved test, the beneficiary could be responsible for the cost.

Protect Yourself

- Beneficiaries should be cautious of unsolicited requests for their Medicare or Medicaid numbers.
- Be suspicious of any unexpected calls or visitors offering COVID-19 tests or supplies. If your personal information is compromised, it may be used in other fraud schemes.
- Ignore offers or advertisements for COVID-19 testing or treatments on social media sites.
- A physician or other trusted healthcare provider should assess your condition and approve any requests for COVID-19 testing.
- If you suspect COVID-19 fraud, contact National Center for Disaster Fraud Hotline (866) 720-5721 or disaster@leo.gov