Donate Safely in Times of Crisis

Center for Cyber Safety and Education

Donating to a cause close to your heart is a great way to get involved and support an organization fighting an issue you're passionate about. Whether it's cyber safety education, a health crisis, a natural disaster or social injustice, donating to nonprofits allows you to make a significant impact from the comfort of your home.

Unfortunately, there are also plenty of options for scammers to trick you into giving your hard-earned money to them instead of a reputable nonprofit. This is especially true when the issues gain national or international attention like the fight against COVID-19, the California wildfires, hurricane relief for major storms like Hurricane Ida or social injustice.

Cybercriminals use the emotional aspect of donating to a worthy cause to scam innocent people by creating fake donation pages. That's why we recommend the following safety measures, which will help you double-check where your donation is going and avoid becoming a victim of fraud.

Here are five tips to help protect your

online gifts:

1. Before making an online gift, use one of these organizations to help you research charities: BBB Wise Giving Alliance, Charity Navigator, CharityWatch, and GuideStar. These resources will help verify the legitimacy of the nonprofit.
2. Be very careful when clicking on links found in emails or on social media. It’s better to open a web browser and go directly to the official website for a charity to make your donation.
3. Thoroughly browse through the charity’s website for key information on donations, such as the organization’s policies on how your money will be used and how your personal information is kept private. Most nonprofits don’t hide what percent of a donation goes directly to programs and services versus administrative and fundraising costs.
4. When giving directly online, be careful how you choose to pay. If you’re prompted to donate by a gift card or money wire, you may have found yourself on an unsafe giving site. So double-check the website you are on. And remember that it’s safest to donate by credit card or check for better fraud protection.
5. Designate exactly where you want your donation to go, even down to a specific program. This will restrict the charity from using the money to fund other ongoing programs, and you can feel better knowing you are donating directly to the cause of your choosing.
6. When donating, make sure you see “HTTPS” (not just HTTP) in the URL. The “S” means the organization is leveraging encryption for its online transactions. Organizations not supporting HTTPS are opening their donors to having their online transactions intercepted.

Don’t let fear of accidentally donating to a scam stop you from doing a great thing for someone else. Just do your due

diligence. If you need more information on identifying various scams and tactics used, check out our free tip sheet **here.**

About the Author: *Patrick "Pat" Craven is the Executive Director of the Center for Cyber Safety and Education. He has more than 35 years of experience in the nonprofit industry and has held various C-Level executive leadership roles across the country at notable charitable organizations such as the Boy Scouts of America (24 years), Big Brothers Big Sisters, and the Vietnam Veterans Memorial Fund in Washington D.C. He is a sought-after speaker and writer on how to keep children and families safe and secure online and is a regular guest on radio, tv and podcast around the world.*