



How to Avoid Charity Scams



Scammers prey on your kindness and often take advantage of tragic disasters. Here's how to donate safely and protect your money.

When a hurricane, flood, wildfire, or other tragic disaster strikes, many people respond with generosity. Unfortunately, cybercriminals respond just as quickly, launching scams that exploit our desire to help.

Furthermore, scammers work every day to take advantage of people's kindness, even when a disaster isn't in the headlines. They will create fake charities and stories to pull your heartstrings and open your wallet.

But with some precautions, you can reduce the chance of falling victim. When in doubt, trust your gut and donate to established, trusted organizations – and only donate through official websites.

1. Fake FEMA websites and impostors

In the wake of hurricanes like Harvey and Irma, scammers posed as government relief agencies to trick victims into sharing personal data or making fraudulent payments.

If you're applying for disaster aid, always go directly to [FEMA.gov](https://www.fema.gov) or [DisasterAssistance.gov](https://www.disasterassistance.gov). Never trust a link sent to you over text or social media.

Red flags for government impostors include:

- Unsolicited emails or phone calls asking for personal info
- Requests for fees to process your FEMA application (FEMA never charges)
- Fake agents showing up in person without official ID

If you're unsure, hang up or stop talking to the person. Call FEMA at 1-800-621-3362 to verify or go to [FEMA.gov](https://www.fema.gov) to donate.

2. Charity scams that prey on goodwill

After a tragic event, we all want to help. But fake charities are common, unfortunately. Some are entirely fake, others mimic real organizations with small but deceptive changes to their names or URLs.

To avoid donating to scammers:

- Research charities at [CharityNavigator.org](https://www.charitynavigator.org)
- Avoid clicking links in emails, ads, or social media posts – go directly to the charity's official website instead

- Never donate via gift cards, wire transfers, or [cryptocurrency](#) (like Bitcoin)

These [scams](#) prey on fear, urgency, and goodwill, which then makes both victims and donors targets.

3. Phony crowdfunding campaigns

Sites like GoFundMe can be lifelines for real victims, but scammers take advantage of them too. Some fake campaigns use stolen images and false stories. Others copy legitimate fundraisers to siphon money from donors.

Before giving to a crowdfunding campaign:

- Only give to campaigns created by people you know or verified sources
- Be cautious of vague campaign descriptions or sketchy organizer profiles

GoFundMe and similar platforms often remove fraudulent campaigns, but it's better to prevent the scam in the first place than to hope for a refund later. GoFundMe has several [resources](#) to [learn more](#).

4. Scam contractors and fake volunteers

Disaster recovery often means home repairs. This opens the door for shady contractors. Some scammers pose as Red Cross workers or contractors offering “urgent” repairs and debris removal services.

How to spot a fake:

- They demand cash upfront or full payment before starting work
- They use high-pressure tactics and don't provide written contracts
- They aren't licensed, have no permanent address, or aren't local

Legitimate contractors will be licensed, insured, and happy to give you references and a written estimate. Be wary of anyone who shows up unannounced offering help for a fee – real volunteers won't charge for tarps or supplies.

5. Sketchy payment requests

Payment apps like Venmo, Zelle, and Cash App are often used in scams because they don't offer much buyer protection. You might see a heart-wrenching story on social media or get a text from someone claiming to collect donations. But once you send the money, there's usually no way to get it back.

Stay safe by:

- Always avoid peer-to-peer payment apps for donations unless you know the person
- Never sending donations via gift cards, wire transfers, or cash
- Focusing on verified campaigns and established organizations

When in doubt, pause and verify. Scammers rely on urgency to cloud your judgment.

Slow down and stay skeptical when you give

Disaster scammers thrive on panic, emotion, and haste. Whether you're donating money or seeking aid, a few moments of verification can protect you and help ensure that your goodwill actually reaches those in need.

Want to support disaster victims safely? Stick to known, verified organizations, and double-check everything before you give. Generosity is a beautiful thing...but only when it lands in the right hands.

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.