Donation and Charity Scams

CONSUMER ADVISORY & PROTECTIVE TIPS

The recent tragic event in Boulder, CO will bring out the best of our communities, but it will also bring forth an opportunity for scammers.

Office of the District Attorney - 18th Judicial District

Proudly Serving Arapahoe, Douglas, Elbert and Lincoln Counties

PEOPLE WANT TO HELP

Tragedy has presented itself in our backyard. The Boulder Community, the State of Colorado, and our nation mourn for our recent loss. As individuals and as a community, we want to help those who were directly impacted. We are touched on many levels and want to reach out.

Tragedies, natural disasters, disease, and the need for basic human services offer the call for people and groups to step up and try to fill the gaps. Donation groups and established charities are there to help in the effort, often by pulling in financial contributions. Scammers are there too, especially when the events are extreme, dire, and overly emotional.

SCAMMERS AT WORK

Fraudsters use the misfortunes of others to take advantage of your kindness and goodwill. Fraud will surface through a range of solicitations, including spoofed communications, copy-cat charity websites, malicious links, heart-wrenching images of victims or devastated landscapes. At times, scammers pretend to be the victim themselves or a family member. The speed and depth of technology, an urgency to act, and your empathy play to their advantage.

TIPS

- **If Donating for Boulder Shooting Relief** - *Visit local Colorado news media and local police department websites for a list of legitimate organizations.*
- **Do Your Own Research on Legitimate Charities and Donation Sites** - *Visit CO Secretary of State website, Charity Navigator, CharityWatch, Better Business Bureau's Wish Giving Alliance.*
- **Never Donate Using** - *Gift Cards, cash, wire transfer, bitcoin. Instead, use credit cards or checks.*
- **Never Give Sensitive Financial or Personal Information** - *Social Security#, driver's license#, bank account#, DOB, etc.*
- **Beware of Unsolicited Communications and Links** - *Don't click on unsolicited emails or LINKS within emails or social media sites like Facebook, Twitter, etc.*
- **Beware Payments Through Crowdfunding Sites** - *During major tragedies and disasters, sites like GoFundMe are not always legitimate. Payments to individuals are generally gifts and not guaranteed tax-deductible donations. See website for details.*
- **Urgency and Pressure to Give** - *Beware requests or demands to donate or act quickly. Reputable charities will not pressure you to make a donation on the spot.*

COMMON RED FLAGS

- **UNSOLICITED Phone Calls, Emails, Texts, Door-to-Door interactions** - *Be careful of organizations, entities or people initiating contact with you.*
- **Sense of Urgency** - *Common scammer tactic. A legitimate charity or cause will always take your donation. End of day urgency to commit or provide is always a red flag.*
- **Non-Traditional Donation Methods** - *Request for donations using Gift Cards, Cash, Wire Transfers, Bitcoin - these types of transactions are difficult to trace. Gift card payment scams are a common issue in Colorado.*
- **Unsolicited Emails with Attachments** - *According to Charity Navigator, it is not typical for legitimate emails from organizations to include attachments.*
- **Being Asked or Feeling Inspired To Donate DIRECTLY Through Social Media Sites** - *Always best to do your homework and investigate on your own. Make sure the group is legitimate and that you are going to charity's legitimate website to make donation.*
- **People That Contact You Online Claiming To Be A Victim** - *Unlikely for a victim of a recent tragedy or disaster to be contacting you directly for assistance. Fraudsters will pose as victims or use their stories and pictures to trick you.*
- **You Receive a "Thank You" For a Donation That You Do Not Remember Making** - *This is an old trick scammers use to relax you into their conversation.*
- **Examine the Web Address** - *Most non-profit web addresses end with .org and not .com.*

SPOOFING

Spoofing is when someone disguises an email address, sender name, phone number, text, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source. Criminals count on being able to manipulate you into believing that these spoofed communications are real, which can lead you to download malicious software, send money, or disclose personal, financial, or other sensitive information. - *FBI.gov*

HELPING LOCALLY

Helping those in need is a good thing. Take the necessary precautionary steps to ensure that your charitable gifts are truly going to those who need it. As for recent events here in CO, research current articles from mainstream news outlets and visit local police department sites to see how you can help.

Contact Consumer Fraud Protection

18th Judicial District

Hotline (720) 874-8547 | consumer@da18.state.co.us