Scam-Proof Donation Checklist (Safety First)

Before you donate (60 seconds):

- **Pause. Any pressure like "donate right now" = red flag.**
- **Ask: Who is this exactly? Get the full organization name, website, and mailing address.**
- **Never donate from a link in a text/email/social post. Type the web address yourself.**

Verify the charity (2–3 minutes):

- **Search the charity name + "review" + "rating."**
- **Confirm the website is real: spelling matches, has a physical address, and clear contact info.**
- **Look for transparency: mission, leadership, how funds are used, and annual reports.**

Safe ways to pay:

- **Use a credit card (best fraud protection).**
- **Use the charity's official website or a verified donation platform.**
- **If donating by check, write it to the organization, not a person.**

Never do these (common scam moves):

- **No gift cards. No crypto. No wire transfers. No cash apps to a personal account.**
- **Don't give bank login info, SSN, or verification codes.**
- **Don't let anyone "pick up" cash or send a courier.**

Smart questions to ask (and how scammers react):

- **"Can you email me the official website and EIN?" (Scammers dodge this.)**
- **"I'll call the charity back using the number on their website." (Scammers hate call-backs.)**
- **"Send me written info; I'll decide tomorrow." (Scammers push urgency.)**

If it's a disaster/emergency fundraiser:

- **Donate only through official org sites (Red Cross, United Way, known local agencies).**
- **Watch for look-alike names and fake social media pages.**

If you already donated and it feels wrong:

- **Contact your card issuer immediately and dispute if needed.**
- **Report the scam to the platform (Facebook/Instagram) and FTC: ReportFraud.ftc.gov.**
- **Tell a trusted family member so they don't get hit next.**

Quick rule to remember:
Pressure + secrecy + unusual payment = scam.