Scamming while scrolling

How online scammers pull at your heartstrings

BETTER BUSINESS BUREAU

It's a hard time right now. There are no two ways about it. People are struggling. We see them come across our timelines — an old man trying desperately to save his dairy farm, a mother trapped in domestic abuse, a child fighting through cancer. On TikTok, these videos often ask viewers to stay for a few seconds and to make a donation. With the sad music, the emotional faces and the tragedy of these stories, we often stop and feel for the people in them.

Unfortunately, many of these videos are fake. Some use AI, while others repurpose video found elsewhere. The posters are not telling their own stories, but they are profiting from them. At the end of the video, or in their profile, they link to a donation page, which is where they capitalize on fake, tragic stories and where sympathetic scrollers can get themselves in trouble.

Once people agree to donate, the scammer on the other end could use that credit card number for anything. They could sell it online, make big purchases themselves or even try to debit the account (a feature many credit card users don't realize they have until it's too late). In the best-case scenarios, the donation simply doesn't make is way to the intended cause and there is no further fraud. In more extreme cases, the donor's personal information is used to commit identity fraud.

To protect yourself, be sure to only give to causes you know or can verify. Verify reputable non-profit organizations by looking up the company name, website and contact information. You can read reviews on bbb.org or ScamTracker. You can also put the organization's name into a search engine with the word "scam". Sometimes, you'll come across reputable organizations whose names or likeness are being ripped off by scammers, which means you may think you're giving to a great cause, but your money is actually going into a criminal's pocket. Be sure the website you're on has the lock icon in the url or has an "s" after "http". Look for any inconsistencies in the url. Some sites will mimic originals by changing a single word or letter.

Be wary of any sites you're sent to directly from social media. It's always a good idea to exit and put the organization's name into a third-party search engine to get more reliable results.

Adobe Stock image

To protect yourself from fraudulent solicitations for donations, be sure to only give to causes you know or can verify.

If you're still unsure, you can pick up the phone and call local non-profits to see what's the best way to give. You can even visit them in-person. This way you'll have a good sense of what they do and who they are before making your gift.

And you should always exercise extra caution while scrolling. It's a tragedy in itself that fraudsters are taking time and money away from people with real and genuine causes. Iif you're unsure and don't want to become a victim yourself, take the extra time to verify where your money is going before you press 'send.'