UNION BANK

FS-ISAC | Security Tips Newsletter

3 October 2025 | Issue No. 25

Be cyber smart to stay cyber safe.

When A Scam Follows a Natural Disaster

Summary

When natural disasters occur, fraudsters are often close behind. Their goal: exploit victims' financial and emotional vulnerability to steal money or personal information.

Types of Schemes

Three different kinds of schemes are typical after a disaster: fraudulent disaster relief charities, post-disaster insurance offers, and repair work.

Charity scams appeal to people's kindness with solicitations – conducted by phone, text, or email – purporting to help victims of a natural disaster.

Post-disaster insurance scams target those victims directly with offers of help – such as "government-provided" temporary housing – for a fee or security deposit on the space.

In a repair scam, scammers pose as contractors offering unsolicited post-disaster repairs on the victim's property. Then they disappear with the down payment. Some do perform repairs, but of far lower quality than they were paid to perform.

Disaster-Related Fraud Schemes

"In 2024, the FBI Internet Crime Complaint Center (IC3) received more than 4,500 complaints representing approximately $96 million in losses from fraudulent charities and disaster relief campaigns."

FBI, 2025 Disaster Fraud Schemes

Red Flags

Consumers should know that representatives of the government (FEMA) do not solicit donations through emails, texts, or phone calls. Government disaster agencies will never call or text to ask for your financial information, and charge no fee to apply for assistance.

Additionally, though time is of the essence after a disaster, scammers manipulate victims by instilling a sense of urgency. Be aware of that technique and remember that your money is better spent if you take the time to verify the recipient's honesty.

Prevention Tips

- **Donate to charities you know and trust** with a proven track record of dealing with disasters. And watch out for name impersonation scams, in which fraudsters use names and logos similar to those of reputable charities. Look twice before you engage, even if the charity seems familiar.
- **Before you give, research the charity yourself** — especially if the donation request comes on social media. Check out the charity on the Better Business Bureau's Give.org, or Charity Watch. Find out exactly how much of your donation will go directly to the people the charity says it helps.
- **Don't donate to anyone who insists you must pay by cash, gift card, money wire, or cryptocurrency**. Legitimate organizations accept ordinary forms of payment. If you decide to donate, write a check directly to the charity, not an individual, or pay by credit card – it will give you more protection.
- **Be cautious about** crowdfunding sites**.** Know that money raised in a crowdfunding campaign goes to the campaign organizer, not directly to the people or cause it's set up to help. Review the crowdfunding platform's policies to be sure it verifies posts aren't scams. And remember, donations to crowdfunded sites aren't tax-deductible.
- **Confirm the number before you donate.** Phone scams often use spoofing techniques to make the information transmitted to your caller ID display appear official. If someone asks you to donate on the phone or via text, call the number on the charity's website to confirm the donation method.
- **Verify that your contractors are legitimate**. Contact your insurance company before hiring anyone, and make sure the company you hire is licensed and bonded.
- **Practice good cyber hygiene.** Most legitimate charity websites end in ".org" rather than ".com" or other extensions. The website https://www.cybercrimeinfocenter.org/ lists common fraud top-level domains (TLD) and ic3.gov-PSA has current information about common scam tactics. Additionally, never click on links or open attachments in unsolicited emails, texts, or social media posts. They can contain malware.

Resources

Learn more about how to donate safely with resources provided by the Federal Trade Commission at ftc.gov/charity. For advice to help you prepare for, deal with, and recover from weather emergencies and the scams that follow, check out ftc.gov/weatheremergencies.

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.gov, law enforcement, and file a report with the Federal Trade Commission.

Getting Help

If you have been the victim of a data breach or loss of your personally identifiable information, or identify suspicious activity involving your financial institution, contact them immediately.

12120 Sunset Hills Rd, Reston
VA 20190