Disaster Tips on Cyber and Social Engineering Scams

Following natural disasters, it is inevitable that "bad actors" will attempt to use the event as a way to scam money for their own pockets. Two types of people are affected; those that were hit by misfortune, and those caring people that desire to help.

Victims are scammed largely by a short list:

- Flood Insurance Robocall Scam
- Job offerings with FEMA in exchange for prepaid application
- Repair, debris removal, and flood mitigation services

The list for charitable persons is larger:

In past disasters, we have seen scams such spoofing the American Red Cross and other organizations. These copycat scams are the most insidious because *often the giver is never aware that the funds go to cybercriminals.*

In addition, charity scams from those that crowdsource, Phish, and use other social engineering skills to cheat do continue to occur following all disasters.

For the wise charitable person, follow the simple rules:

- **Donate to charities you know and trust** with a proven track record with dealing with disasters.
- **Be alert for charities that seem to have sprung up overnight in connection with current events.**Check out the charity with the Better Business Bureau's (BBB) Wise Giving Alliance, Charity Navigator, Charity Watch, or GuideStar.
- **Designate the disaster** so you can ensure your funds are going to disaster relief, rather than a general fund.
- **Never click on links or open attachments in e-mails unless you know who sent it.** You could unknowingly install malware on your computer.
- **Don't assume that charity messages posted on social media are legitimate**. Research the organization yourself.

- **When texting to donate, confirm the number with the source before you donate.** The charge will show up on your mobile phone bill, but donations are not immediate.
- **Find out if the charity or fundraiser must be registered in your state** by contacting the National Association of State Charity Officials. If they should be registered, but they're not, consider donating through another charity.
- **Do not follow unsolicited web links in email messages**.
- **Use caution when opening email attachments**. Refer to the US-CERT Tip Using Caution with Email Attachments for more information on safely handling email attachments.
- **Keep antivirus and other computer software up-to-date.**
- **Refer** to the Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.
- **Verify the legitimacy of any email solicitation** by contacting the organization directly through a trusted contact number. You can find trusted contact information for many charities on the BBB National Charity Report Index

Please reference the US-Cert and FTC for further information

US-CERT

https://www.us-cert.gov/ncas/current-activity/2017/08/28/Potential-Hurricane-Harvey-Phishing-Scams

Federal Trade Commission (FTC)

https://www.consumer.ftc.gov/blog/2017/08/wise-giving-wake-hurricane-harvey