August 2017

Protecting yourself from potential scammers while being charitable

The states of Texas and Louisiana are reeling from the devastating impact of Hurricane Harvey, and members of the public are eager to do whatever they can to try to help. But as is too often the case when tragedy strikes, the public needs to be alert for charity relief scams that prey on public sympathies in order to steal private information and ultimately, funds intended for Harvey relief. Scammers are fraudulently collecting sensitive information and stealing donations by creating and using fake social media platforms (e.g., Facebook, charity websites, phishing email, and twitter) to ask for donations to the Hurricane Harvey Relief funds. These fake websites will usually do one of two things: 1) ask for a credit card number to steal the donations or 2) infect your electronic device with malicious software that can extract sensitive information (passwords, usernames, or account numbers) that is subsequently used to commit fraud.

Scammers' using natural disasters to take advantage of charitable individuals is not a new cybersecurity issue. In 2005, the American Red Cross asked the FBI to investigate at least 15 fake websites that were created to look like legitimate Red Cross posts for Hurricane Katrina donations. In 2012, a charity calling itself the "Hurricane Sandy Relief Effort" purportedly raised $600k for storm victims, but it was all actually a scam to help the thieves pay off their own credit card debt.

Want to help? Here are some tips!

- If you want to make a donation, go to the charity's official website to make the donation. Type the address in your browser or use a bookmark to ensure you don't go to a fraudulent website by mistake.
- Be sure to verify the existence and legitimacy of non-profit organizations by using Internet-based resources. You can find trusted contact information for many charities on the BBB National Charity Report Index. [i]
- Most legitimate charities maintain websites ending in ".org" rather than ".com".
- Do not respond to any unsolicited incoming e-mails or text messages, by clicking links or downloading files contained within those messages, because those links or files may contain viruses or other malicious software (including ransomware) that could steal your personal information and/or harm your computer or other electronic device.

- Be cautious of organizations with copycat names similar to but not exactly the same as those of reputable charities.
- Do not be pressured into making contributions; reputable charities do not use coercive tactics.
- Legitimate charities do not normally solicit donations via money transfer services.

To combat the threat of this type of scam, **HIPAA Covered Entities (CE) and Business Associates (BA)** should consider training staff on the following good practices:

- Hang up the phone if you are suspicious of the caller.
- Never allow remote access to your computer unless such access is known to be legitimate, and the requestor's authenticity can be verified (e.g., calling your IT Help Desk to verify the identity of IT support personnel requesting remote access to perform maintenance).
- Do not trust unsolicited phone calls, emails, or texts.
- Be suspicious of requests for personal information over telephone, email, or text.
- Do not download unknown software or purchase unsolicited online services.
- Verify the identity of the caller directly with CE or BA officials, or with the company the caller claims to represent.
- Record the caller's information if you suspect a scam and report it in accordance with your organization's policies.

The **Federal Trade Commission** (FTC) recommends avoiding any charity or fundraiser that [ii]:

- Refuses to provide detailed information about its identity, mission, costs, and how the donation will be used.
- Won't provide proof that a contribution is tax deductible.
- Thanks you for a pledge you don't remember making.
- Guarantees sweepstakes winnings in exchange for a contribution. By law, you never have to give a donation to be eligible to win a sweepstakes.

Resources:
FEMA: https://www.fema.gov/news-release/2016/05/11/be-alert-disaster-related-fraud-and-scams
Office for Civil Rights (OCR): https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/index.html
Better Business Bureau (BBB) Scam tracker: https://www.bbb.org/scamtracker/us

[i] http://give.org/charity-reviews/national
[ii] https://www.consumer.ftc.gov/features/feature-0011-charity-scams