Health Information Compliance Alert

Enforcement News: Social Engineers Take Advantage of Hurricane Turmoil

Tip: Verify the charity before you offer assistance.

Con artists always know to strike when the irons are hot. And with Hurricane Harvey and Irma tragedies promoted across numerous media outlets, hackers and criminals are ready to make an easy buck.

"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," noted the OCR's Cybersecurity Newsletter in its August 2017 edition.

The monthly report suggests that the social engineers use fake websites, online phishing scams, telephone calls, and more to lure unsuspecting folks into handing over their personal information and their money. "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," the OCR guidance said.

The OCR offered advice on what to do if you think you've been hacked or the victim of a charity social engineering attack. It also suggested investigating fully the organization before you send your check, give out your credit card details, or fork over your personal history.

To read the OCR's Cybersecurity Newsletter, visit https://www.hhs.gov/sites/default/files/august-2017-ocr-cyber-newsletter.pdf.