Codify
BY AAPC

Health Information Compliance Alert

Cybersecurity: Pocket This Charity Advice to Sidestep Scams

Tip: Do your research before your practice donates cash.

Helping a worthy charity or bolstering a struggling community in the aftermath of a disaster is important. Charitable contributions promote the spirit of giving - and represent the foundation of the healthcare industry. However, not every email request is on the up-and-up, and that's why it's critical to do your homework before you give out sensitive practice information.

Review: Dating as far back as Hurricane Katrina in 2005, the Federal Bureau of Investigation (FBI) started noticing fake websites and charities popping up after disasters. The scammers preyed on unsuspecting victims, stealing private data, according to a Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Cybersecurity Newsletter report.

In the wake of such terrible 2018 disasters as Hurricanes Florence and Michael and the California wildfires, covered entities (CEs) should prepare for social engineering schemes. Also, during the holiday season, when practices are more likely to have their guards down and give to charities, the activities of hackers and social engineers only increases.

Consider this OCR advice before you donate and hand out credit card information and sensitive data:

- Check to see if the charity has an official website.
- Scour the Internet for details and a backstory on your chosen charity before you hit send on your donation to ensure its legitimacy.
- Look for ".org" versus ".com." According to OCR, "most legitimate charities maintain websites ending in '.org' rather than '.com'.".
- Watch for phishing schemes masquerading as charities or relief efforts. These types of emails often come with viruses that invade your systems or mobile devices using malware.
- Research the name, especially if it is similar to a local organization or a "copycat" of a reputable firm, stresses the Cybersecurity Newsletter guidance.
- Ignore suspicious charity requests for personal or practice information via email, text, or phone.
- Don't open attachments or download "unsolicited online services," warns the OCR.
- "Verify the identity of the caller" and "record the caller's information if you suspect a scam and report it in accordance with your organization's policies," the Cybersecurity Newsletter advises.

Reminder: "Social engineering tactics are designed to obtain secure information (login, customer, patient, or corporate data) by conning a person into revealing the information," explains **Michael Whitcomb,** CEO of the IT security and regulatory compliance firm **Loricca** in Tampa, Florida. These types of attacks exploit the overly trusting nature of most people. But remember with a combination of training, concrete policies, and skepticism, social engineers can be stopped in their tracks.

Resource: Review the OCR's Cybersecurity Newsletter at www.hhs.gov/sites/default/files/august-2017-ocr-cyber-newsletter.pdf.