The Monthly Security Awareness Newsletter for You

Charity & Disaster Scams

Cyber criminals know that one of the best ways to rush people into making a mistake is by creating a heightened sense of urgency. And one of the easiest ways to create a sense of urgency is to take advantage of a crisis. This is why cyber criminals love it whenever there is a traumatic event with global impact. What most of us regard as a tragedy, cyber criminals view as an opportunity, such as the breakout of a war, a major natural disaster such as a volcanic explosion, and of course infectious disease breakouts like COVID-19. When there is an immense amount of social media and news coverage about a certain event, cyber criminals know that is the time to strike.

They use this opportunity to create timely phishing emails or scams about the event, and then send that phishing email or launch the scam to millions of people around the world. For example, during a natural disaster, they may pretend to be a charity asking for donations to save children in need. Cyber criminals can often act within hours of a crisis or disaster, as they have all the technical infrastructure prepared and are ready ahead of time. How can we protect ourselves the next time there is a big crisis or disaster, and cyber criminals seek to exploit it?

How to Detect and Defend Against These Scams

The key to avoiding these scams is to be suspicious of anyone who reaches out to you. For example, do not trust an urgent email claiming to be from a charity that desperately needs donations, even if the email appears to be from a brand that you know and trust. Do not trust a phone call claiming to be a local food bank pressuring you to donate. The greater the sense of urgency, the more likely the request is an attack. Here are some of the most common indicators of a charity scam:

- Be very suspicious of any charity that requires that you donate via cryptocurrency, Western Union, wiring money, or gift cards.
- Cyber criminals can change their caller ID phone number to make their phone call look like it's from your local area code or from a trusted name. Caller ID cannot be relied upon these days.
- Some cyber criminals will use names and logos that sound or look like a real charity. This is one reason it pays to do some research before giving.
- Cyber criminals will often make lots of vague and sentimental claims about what they will do with your money but give no specifics about how your donation will be used.
- Do not assume pleas for help on crowdfunding sites such as GoFundMe or social media sites such as TikTok are legitimate, especially in the wake of a crisis or tragedy.
- Some cyber criminals may try to trick you into donating to them by thanking you for a donation you made in the past when, in reality, you never donated to them.

- Do not give out personal or financial information in response to any unsolicited request.

How to Make a Difference Safely

To donate in times of need or to help those impacted by a disaster, donate only to well-known, trusted organizations. You initiate the connections and decide who to reach out to, such as what websites to visit or what organizations to call. When you consider giving to a charity, search its name plus words like "complaint," "review," "rating," or "scam." Not sure which charities to trust? Start by researching on government websites you trust, or perhaps links provided by a well-known and highly trusted news organization. Donating in times of need is a fantastic way to make a difference, just be sure you are giving to legitimate organizations.

Guest Editor

Dr. Jessica Barker is an award-winning leader on the human side of security. She is the co-CEO of Cygenta and a bestselling author. Jessica is on the SANS Security Awareness Summit advisory board.

Resources

FTC Charity Fraud: https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams
Social Engineering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Top Three Scams: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Messaging Attacks: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Phone Call Attacks: https://www.sans.org/newsletters/ouch/vishing/
Charity Navigator: https://www.charitynavigator.org/