NIGC Tech Alert

VIGILANT GIVING: DO NOT BE A VICTIM OF A MALICIOUS CYBER ATTACK

During the first nine months of 2023. the U.S. experienced the highest number of devastating natural disasters on record for a single year. These 23 disasters in the first nine months alone included flooding, wildfire, winter storms, tornadoes, and hurricanes have caused loss of lives, billions of dollars in damages, and ripped the hearts of generous citizens around the country that are moved to support disaster relief efforts. Financial donations are great ways to contribute to such efforts and technology makes it convenient to financially support a charity of choice. Unfortunately, the internet is infested with bad actors seeing these disasters as opportunities to exploit any lack of vigilance. Whether utilizing a fundraising app, a website (e.g., GoFundMe, IndieGoGo), or donating funds through an established non-profit (e.g., UNICEF, Doctors Without Borders), ***always, be vigilant.*** Those with malicious intent restlessly seek opportunities to steal charity contributions, access Personal Identifiable Information (PII) of donors, and perform other malicious activities to exploit good intentions.

The NIGC Office of Cybersecurity partners with the Cybersecurity and Infrastructure Security Agency (CISA) to elevate our internal cybersecurity practices to higher standards. The NIGC Chief Information Security Officer, Abner Desir, stated, "CISA reminds us of the need for heightened awareness as our kind and generous hearts move us to assist victims of natural weather disasters like hurricanes, floods, and wildfire events." CISA recommends IT users to remain alert against malicious cyber activity, especially following natural disasters because attackers target disaster victims as well as donating citizens by leveraging social engineering tactics, techniques, and procedures (TTPs). Social engineering TTPs include using threat actors posing as trustworthy persons or organizations like disaster-relief charities to solicit personal information via email or malicious websites. CISA recommends exercising extreme caution in handling emails with disaster-related subject lines, attachments, and hyperlinks. In addition, be leery of social media requests and text messages related to weather disaster events.

NIGC and CISA encourages users to review the following resources to aid in avoiding falling victim to malicious cyber activity:

- Federal Trade Commission's Staying Alert to Disaster-related Scams: https://consumer.ftc.gov/features/dealing-weather-emergencies#stayingalert
- Before Giving to a Charity: https://consumer.ftc.gov/articles/giving-charity
- Consumer Financial Protection Bureau's Frauds and scams: https://www.consumerfinance.gov/consumer-tools/fraud/
- CISA's Using Caution with Email Attachments https://www.cisa.gov/news-events/news/using-caution-email-attachments
- Avoid Social engineering and Phishing Attacks https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

Contact Us: ocio@nigc.gov