

[Home \(https://www.bleepingcomputer.com/\)](https://www.bleepingcomputer.com/) > [News \(https://www.bleepingcomputer.com/news/\)](https://www.bleepingcomputer.com/news/)

◀ 71

> [Security \(https://www.bleepingcomputer.com/news/security/\)](https://www.bleepingcomputer.com/news/security/)

> 'Help Ukraine' crypto scams emerge as Ukraine raises over \$37 million

'Help Ukraine' crypto scams emerge as Ukraine raises over \$37 million

By

March 1, 2022

07:51 AM

0

Ax Sharma

(<https://www.bleepingcomputer.com/author/ax-sharma/>)



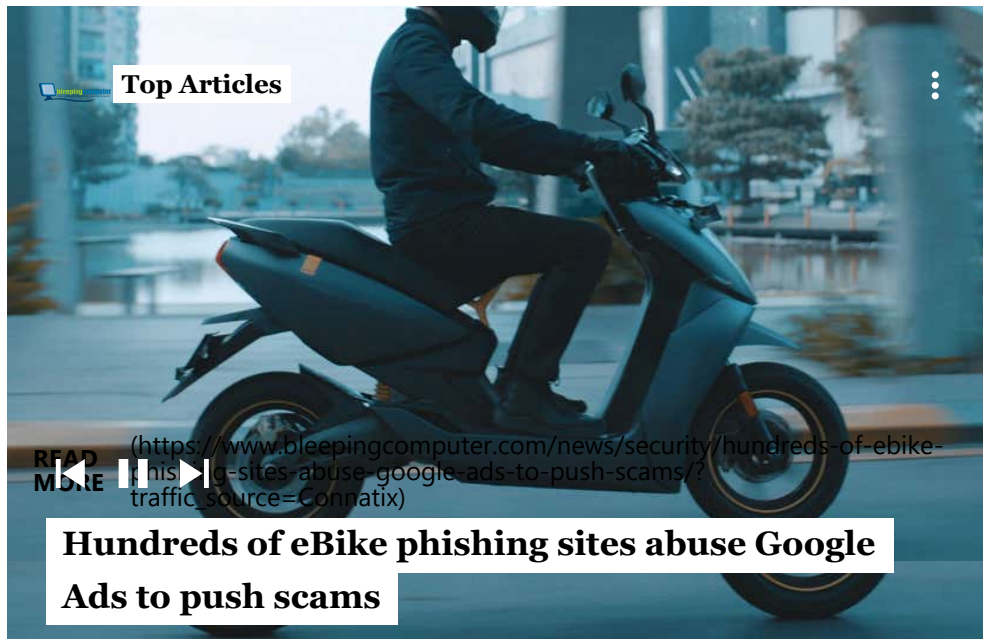
Scammers are now targeting unsuspecting users via phishing webpages, forum posts, and email links enticing users to "help Ukraine" by donating cryptocurrency.

The development follows Ukraine's successful effort of raising over \$37 million in crypto donations from all around the world amid the country's ongoing invasion by Russian troops.



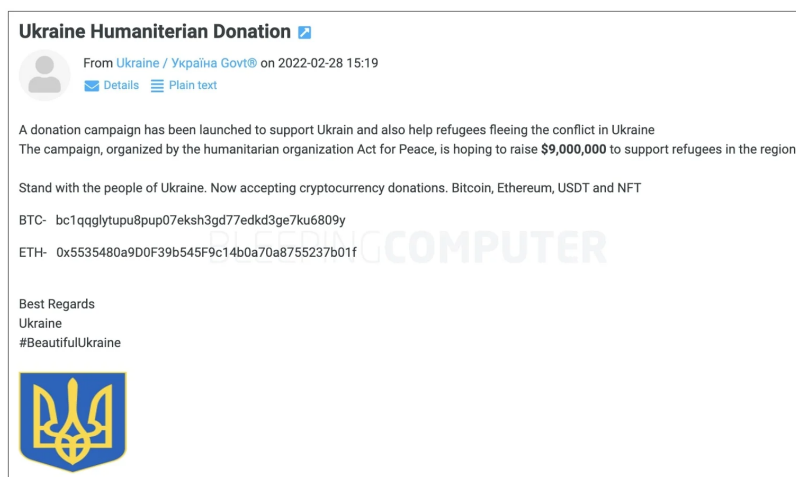
'Help Ukraine' crypto donation scams on the rise

This week BleepingComputer has come across a series of cryptocurrency scams enticing users to "help Ukraine" by donating to counterfeit Bitcoin and Ethereum addresses that are not affiliated with the Ukrainian government.



To facilitate this phishing campaign, attackers are using a variety of means—from phishing emails that appear to originate from *npr.org* or the United Nations Office for the Coordination of Humanitarian (OCHA) domains, to posting forum posts claiming to be behind the "Help Ukraine" movement.

One such phishing email, among others reviewed by BleepingComputer, is shown below:



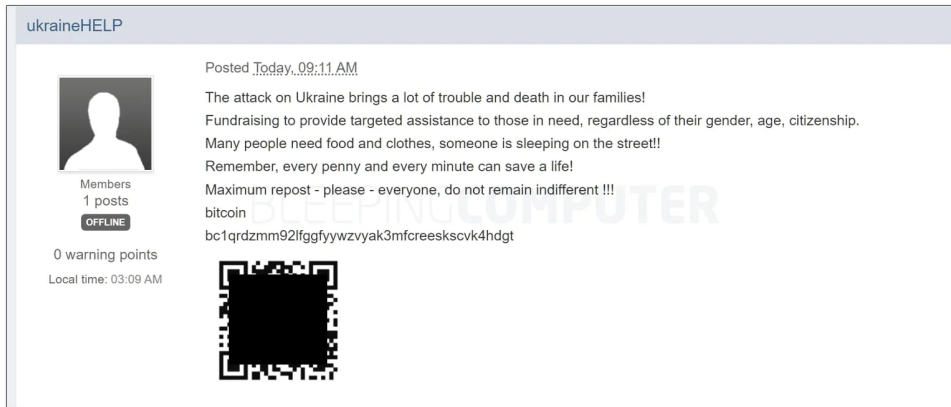
"Help Ukraine" phishing email pretending to come from *npr.org* (BleepingComputer)

Additionally, BleepingComputer came across a forum post shared on one of the forum threads that we have since taken down.

"The attack on Ukraine brings a lot of trouble and death in our families! Fundraising to provide targeted assistance to those in need, regardless of their gender, age, citizenship," reads the forum post.

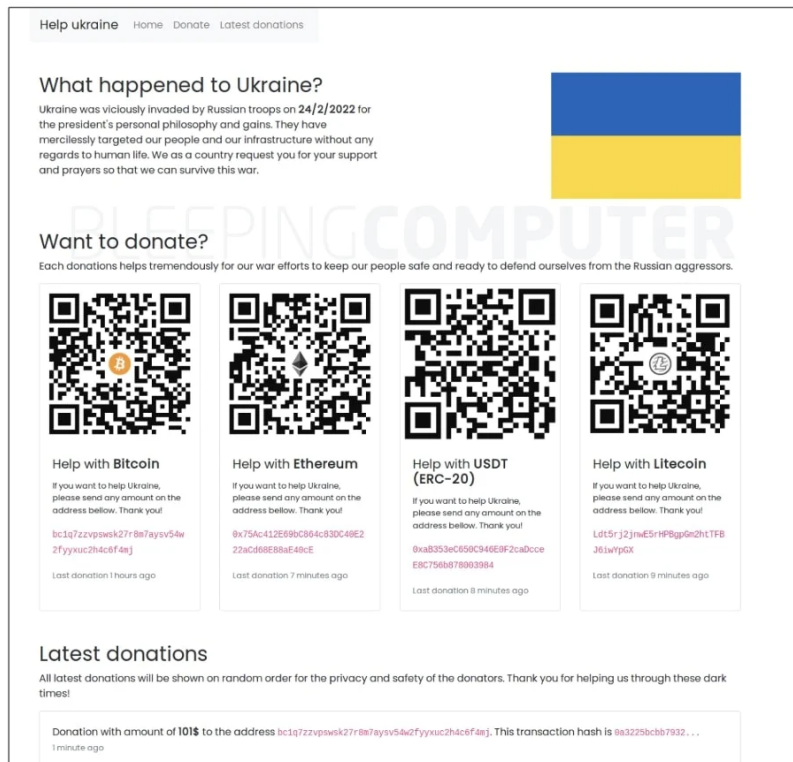


"Many people need food and clothes, someone is sleeping on the street!!
Remember, every penny and every minute can save a life!"



Counterfeit 'Help Ukraine' forum post (BleepingComputer)

Ransomware intel provider *MalwareHunterTeam* also came across (https://twitter.com/malwrhunterteam/status/1498232484055719939?) .or g domains set up by scam artists looking to con prospective donors, as did others:



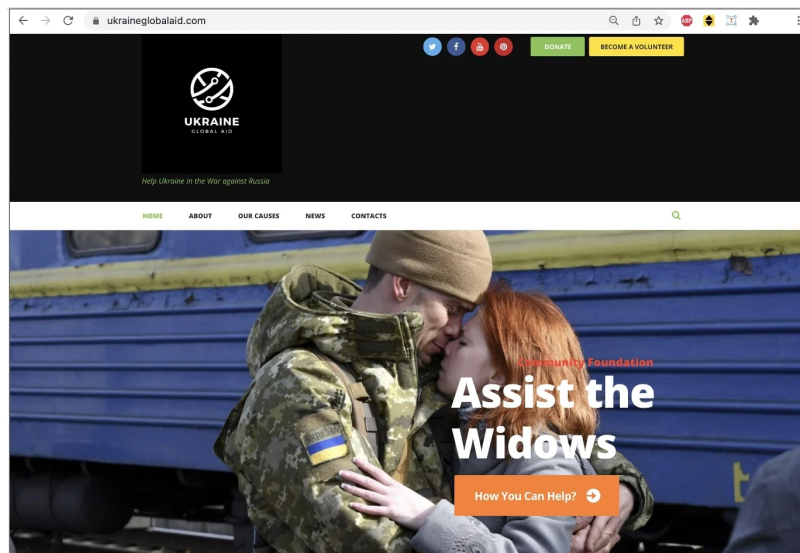
Counterfeit ukraine-donate[.]org domain set up by scammers (BleepingComputer)





More fraudulent donation websites reported by @JCyberSec_ (Twitter
(https://twitter.com/JCyberSec_/status/1498239774116753409))

Cybersecurity researcher Jake (http://twitter.com/JCyberSec_) also shared with BleepingComputer a dubious donation site "UkraineGlobalAid.com" that could fool some on a first glance but contains broken links all over:



Fraudulent Ukraine fundraising site UkraineGlobalAid[.]com

What makes these scams particularly dangerous is their appeal to emotion that unwary recipients may not be able to resist, especially at a moment of need for Ukraine.



The fact that the government of Ukraine is actively seeking crypto donations in Bitcoin, Ethereum, and other forms of crypto from all over the world may inadvertently lend credibility to such scams.

Ukraine raises over \$37 million in crypto donations

In what can be described as the first-ever large-scale crypto crowdfunding effort from a national government, Ukraine has thus far raised over \$37 million

(<http://bitcoin%20%28btc%29%2C%20ether%20%28eth%29%2C%20tether%20%28usdt%29%20and%20other%20altcoins/>) in Bitcoin (BTC), Ether (ETH), Tether (USDT), and other altcoins. Additional donations worth \$13 million are expected to arrive as the country battles an ongoing crisis.

Last week, after Russia's unprovoked attack on Ukraine, the Ukrainian government made a crowdfunding appeal to the world seeking cryptocurrency donations.

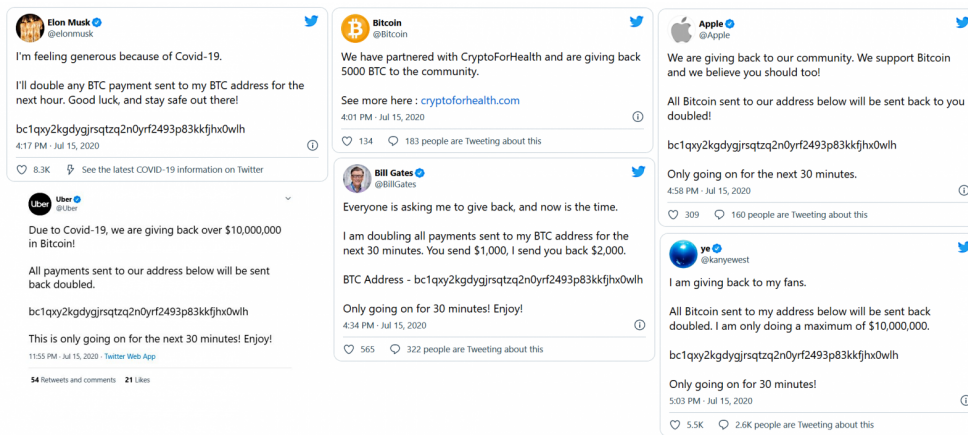
In a tweet posted by the official Twitter account of Ukraine, government officials shared the authentic Bitcoin and Ethereum addresses where funds could be sent to:



This may have raised eyebrows among netizens suspecting (<https://twitter.com/TomStri68606037/status/1497595399841804288>) if Ukraine's official Twitter account had been hacked—and for good reason.

In 2020, attackers had hijacked verified Twitter accounts (<https://www.bleepingcomputer.com/news/security/apple-kanye-gates-bezos-more-hacked-in-twitter-account-crypto-scam/>) of prominent public figures and companies including Elon Musk, Bill Gates, Kanye West, and Apple, to promote "double your cryptocurrency" scams:





Hijacked Twitter accounts of public figures promoting crypto scams in 2020 (BleepingComputer)

In 2021, Bitcoin.org was hacked with attackers having successfully stolen \$17,000 from unwary users (<https://www.bleepingcomputer.com/news/security/bitcoinorg-hackers-steal-17-000-in-double-your-cash-scam/>) in a similar scam.

It's tempting to dismiss these scams thinking no one falls for them, but, similar crypto scams have been hugely successful and generated hundreds of thousands of dollars in the past.

For example, in 2018 crypto scammers had made \$180K (<https://www.bleepingcomputer.com/news/security/fake-elon-musk-twitter-bitcoin-scam-earned-180k-in-one-day/>) in a single day. In 2021, Twitter suffered a massive attack with threat actors walking away with \$580K (<https://www.bleepingcomputer.com/news/security/verified-twitter-accounts-hacked-in-580k-elon-musk-crypto-scam/>) in a week. And, in February last year, we saw another incidence of crypto scammers making at least \$145,000 (<https://www.bleepingcomputer.com/news/security/twitter-scammers-earned-over-145k-this-week-in-bitcoin-ethereum-doge/>).

However, subsequent tweets [1 (<https://twitter.com/TomicahTD/status/1497601610775769094>), 2 (<http://twitter.com/FedorovMykhailo/status/1497549813205848068>)] from Ukrainian First Vice Prime Minister, Mykhailo Fedorov, have confirmed the government's ask was legitimate.

For those looking to donate to Ukraine, make sure to only use the official wallet addresses published by the Ukrainian government ([http://twitter.com/Ukraine/status/1497594592438497282?](http://twitter.com/Ukraine/status/1497594592438497282?ref_src=twsrc%5Etfw) ref_src=twsrc%5Etfw) and refrain from engaging with any suspicious donation emails or social media posts.

Updates (times in ET):

