CNC Intelligence Warns that Scammers are Using Misspelled Cryptocurrency URLs to Steal Crypto

WASHINGTON, DC, UNITED STATES, December 14, 2021 / EINPresswire.com/ -- Misspelled Cryptocurrency URL sites are created to dupe internet users attempting to reach legitimate cryptocurrency sites such as Blockchain.com. Blockchain is a cryptocurrency buying and selling site. There exists big money in these minor typos. According to leaked sale records after a hack of Epik, a man in Brazil paid an excess of 200,000 dollars' worth of bitcoin between last November and February for typo

addresses. Epik is an internet services company that hosts far-right and other extremist sites. The Brazilian-based man also purchased 16,000 dollars' worth of these typos to mimic Coinbase, another cryptocurrency exchange.

Avoid Being Scammed!

Be careful not to fall victim to these Cryptocurrency scams. Learn how to distinguish between a genuine and fictitious website. Although one may be following a lead from a cryptocurrency expert, they may still fall victim to a fake site. Numerous fictional websites which resemble original cryptocurrency sites and good cryptocurrency companies have emerged.

One should rethink and delve deeper into the website if they notice the small lock icon and the HTTPS are missing in the site address. Both these features found near the URL are security features.

It can also be that the site they are visiting mirrors the original, barring the payment option. For instance, if a website looks legit for, however, the company is not familiar, it may in fact be a phishing site, designed to look like a legitimate site. It is even possible that the site is an almost perfect copy of a real and legitimate website. One trick fraudsters use is to replace the letter "o"

with "0" to create a counterfeit URL. Such a platform will not lead to the correct Cryptocurrency investment site the visitor researched but will direct to a fraudulent site.

These web addresses, sometimes called domains, come at a high price. This leads someone to think that he will make a substantial profit—domains ending in dot-com cost approximately 10 dollars annually. However, scammers often target cheaper domains.

What are Experts Saying?

According to [Nick Nikiforakis](#), there exists a genuine monetization chance. Nick Nikiforakis is a science professor at Stony Brook University. He has studied phishing, the process of using resembling websites to steal passwords. He states that if someone steals another person's credentials, they can transfer the other person's bank account funds immediately.

It is hard to recover funds if this happens, said Nikiforakis. This is because cryptocurrency transactions are semi-anonymous and without professional experience and tools it can be extremely difficult to identify the individuals behind the transactions. [The experts at CNC Intelligence](#) urge the public to do due diligence before sending cryptocurrency to any unknown third party. While it takes a few moments to send cryptocurrency, the process of tracing the cryptocurrency, obtaining the identity of the beneficiary of the transaction, and tracking down the real people behind the cryptocurrency can take months.

In conclusion, it is essential to know that cryptocurrency scams exist, and they can cost victims a lot. It is, therefore, crucial to learn how to differentiate a legit cryptocurrency website or company from a fake one. Before using any website to invest online you should also verify that the website is the official website of the company and that the company is a legitimate company. Investors should also be wary of cryptocurrency websites or companies they don't know before interacting with them. It is also advisable to seek professional advice which can assist investors to be able to discern between legitimate websites and fictitious sites, designed to defraud the public.

Elliot Taylor
CNC Intelligence Inc.
+1 202-773-4704
[email us here](#)

This press release can be viewed online at: https://www.einpresswire.com/article/557523960