Bitcoin Investment Scams, Investigated!

Author	josh
Date	2020-12-04 23:02:53

Overview

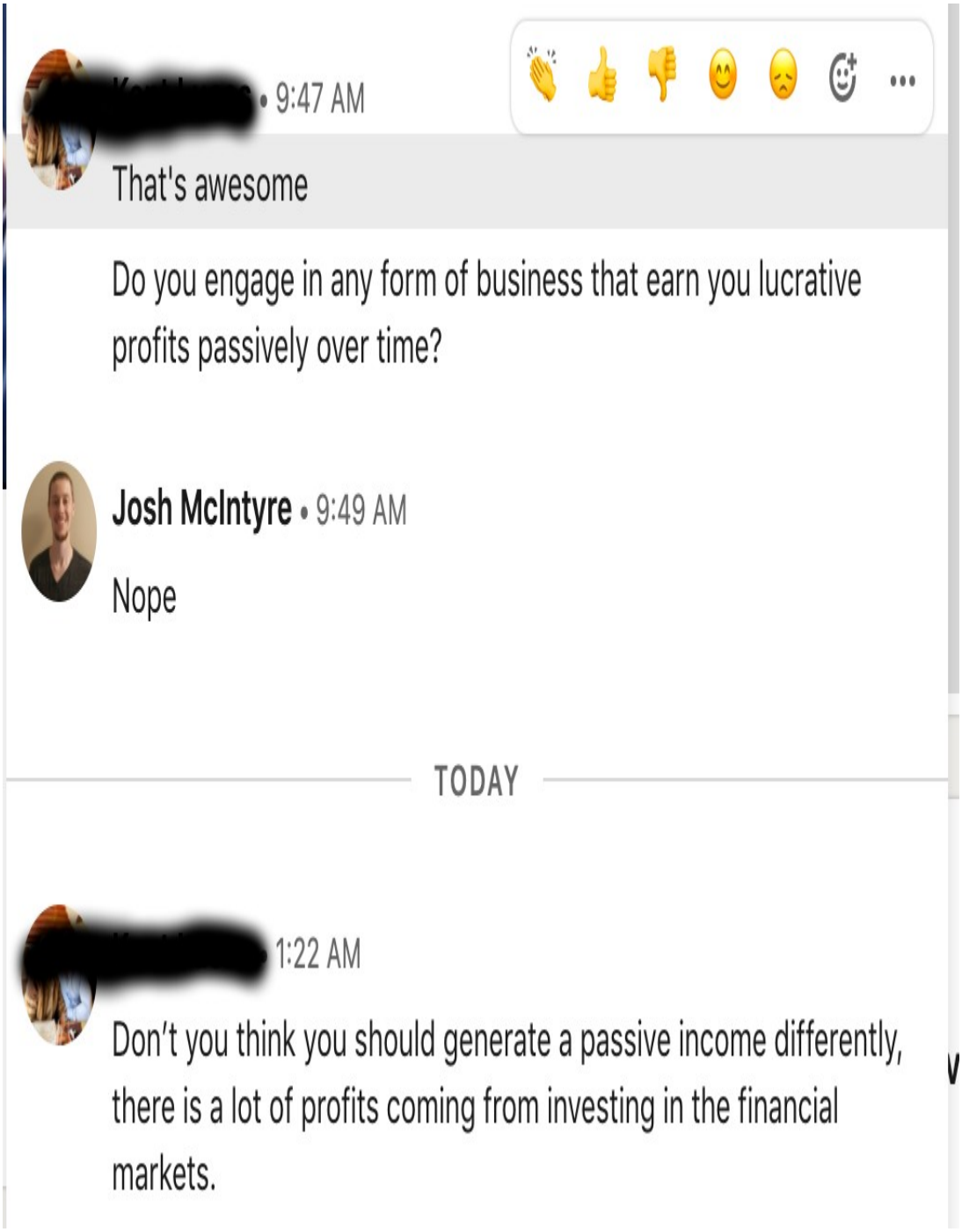
I *hate* scammers, don't you? Investment related scams are nothing new, and Bitcoin related investments scams aren't exactly new either at this point. It may seem obvious to some, but people do in fact fall for these scams - and it's *not* because they are stupid.

Scammers use particularly insidious skills to mark and convince their prey called *social engineering*. I get contacted by these thieves all the time, and so I decided to play along with one and show you the lengths that social engineering scammers will go to in order to convince their victims.

Social Engineering Techniques, and How to Spot Them

The Cold Contact

The first sign of something fishy came in how this individual chose to contact me in the first place - completely out of the blue. I was contacted by the stranger via the professional social networking site LinkedIn. This person asked a few little "butter me up" questions and then got right to asking if I look for "lucrative passive investment opportunities".



Oh boy, a passive investment opportunity! Do you detect my sarcasm?

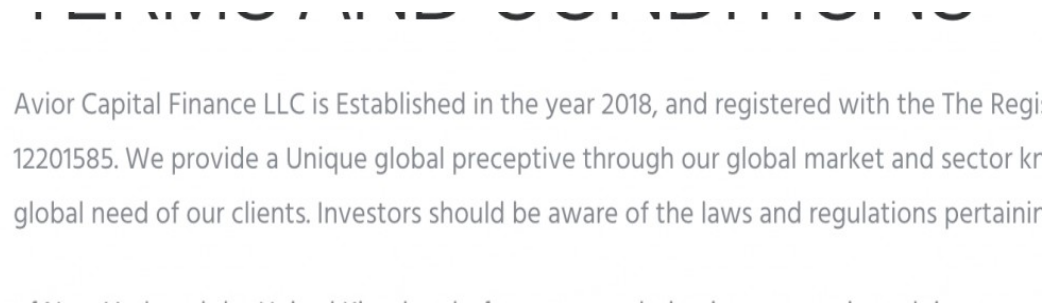
This right here is a first sign to be aware of. No one contacting you out of the blue with an "investment" opportunity wants to help you out of the goodness of their own heart. Quite the opposite, in fact. If it is not an outright scam, they are at the very least *trying to sell you something.* So look out for this.

Misrepresenting Themselves - Fake Persona, Fake Credentials

I even tried to, at first, call this scammer out on his scheme. I knew this was a scam from the get go, but scammers are often prepared for initial objections. This person sent me links to a legitimate company and the certifications of the person he was *pretending to be!* This is another thing to look out for - look very closely and carefully at who a person claims to be representing.

This person pretended to be a legitimate, registered financial professional working for a legitimate company called Avior. However, upon closer inspection, the founding date of the *real* Avior and the *fake* Avior are totally different! And of course, this person simply pretended to be another person - quite easy to do on the internet.

The Real Avior Capital, founded 2005 - direct from the Bloomberg link the scammer sent me

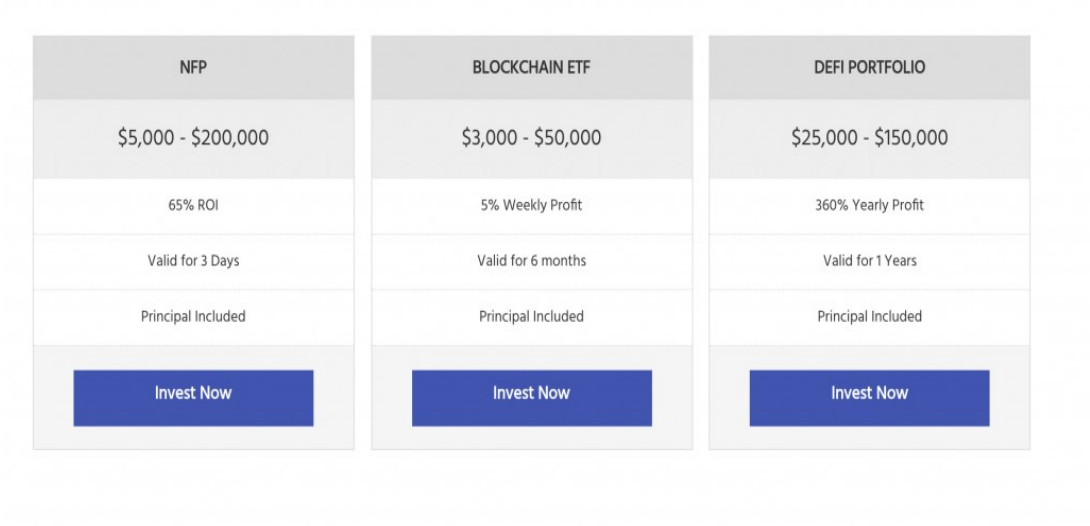


The scam Avior website says founded in 2018...interesting

Fake, But Convincing Websites

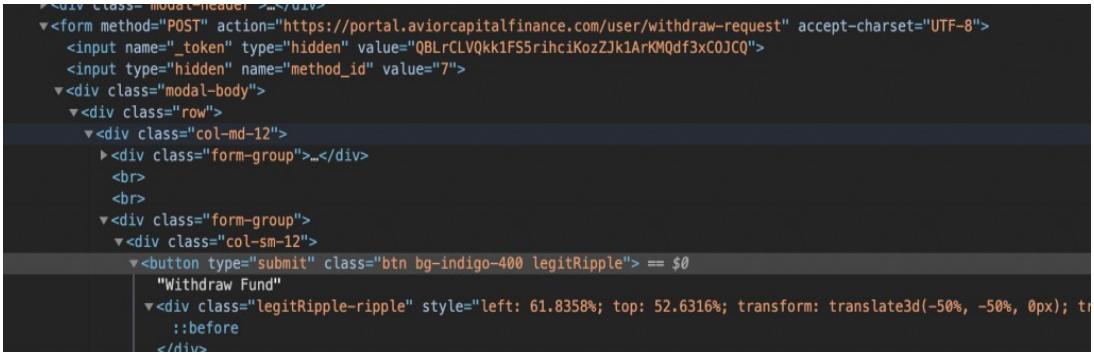
Anyone can create a website. *Anyone*. In fact, chaintuts.com was created and maintained by a very normal person with no magical abilities...

Look *very* closely at fake website links sent to you. This website used HTTPS (the little lock in your browser address bar) and a very modern look-and-feel!



Modern web layout on the fake website

However - it turns out that this website *doesn't actually do what it say it does*. Upon closer inspection, I noticed that the code of the withdraw function doesn't actually do anything other than generate some convincing messages. This simple web form doesn't do anything more than pretend it has some reason you can't withdraw your funds.

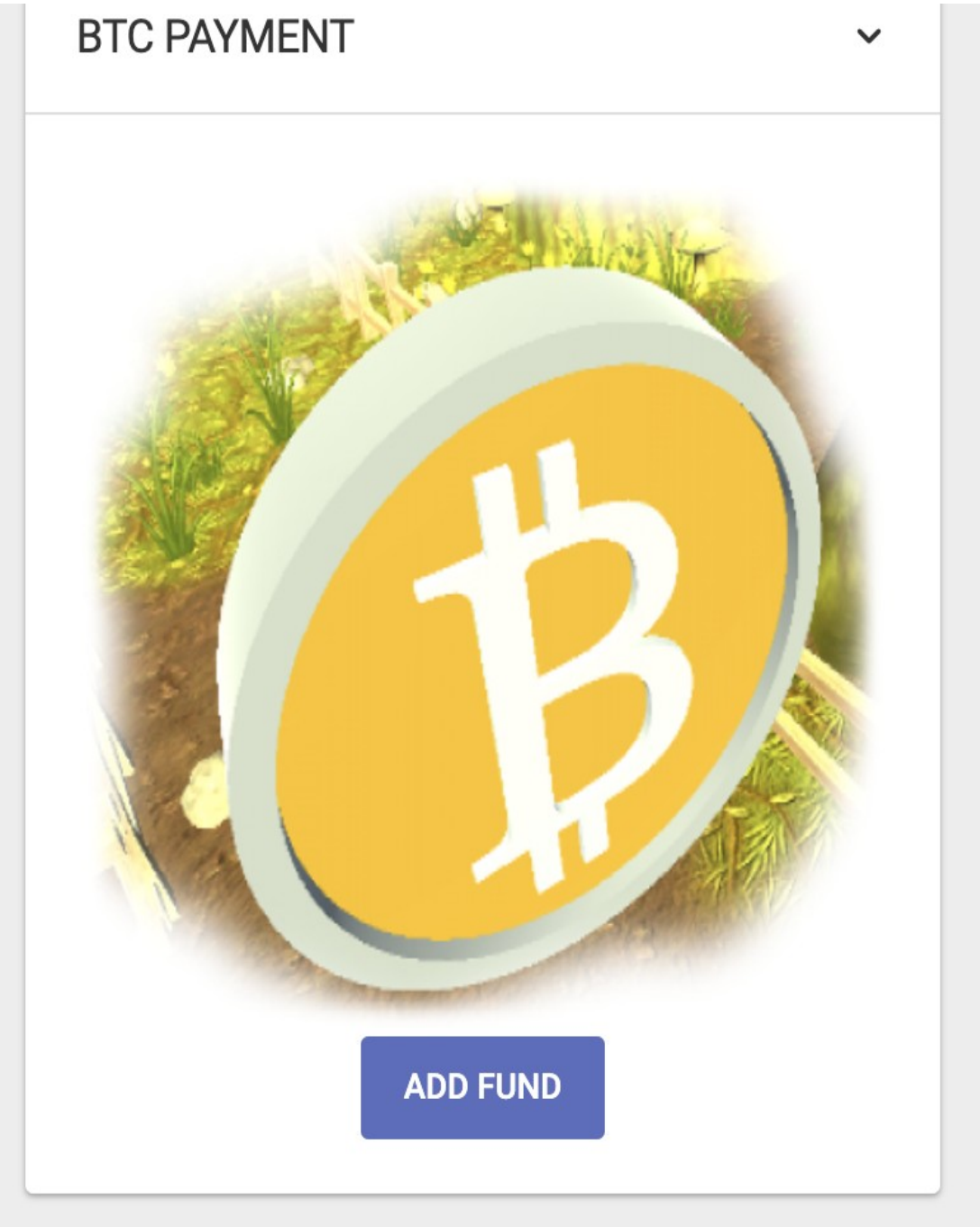


A simple web form, no real withdrawals here

Now looking at the client-side code isn't really the answer here - this is just some extra tinkering I did to help show you all how these websites can *look* convincing. You need zero software engineering skills to spot a fake, in fact. The real thing to look for is in the "payment options".

I noticed that the only way to make a deposit in this totally legitimate investment site is via Bitcoin. Now *that* is suspicious. I surely do want to see worldwide adoption of Bitcoin, but in reality most major investment companies aren't using it yet. And they *certainly* are not using it as the only deposit option available. The reason scammers love Bitcoin is because transactions are *irreversible by design, as a security feature.* They don't want you to use a credit card because you can do a chargeback. With Bitcoin, they can simply take your money and run.

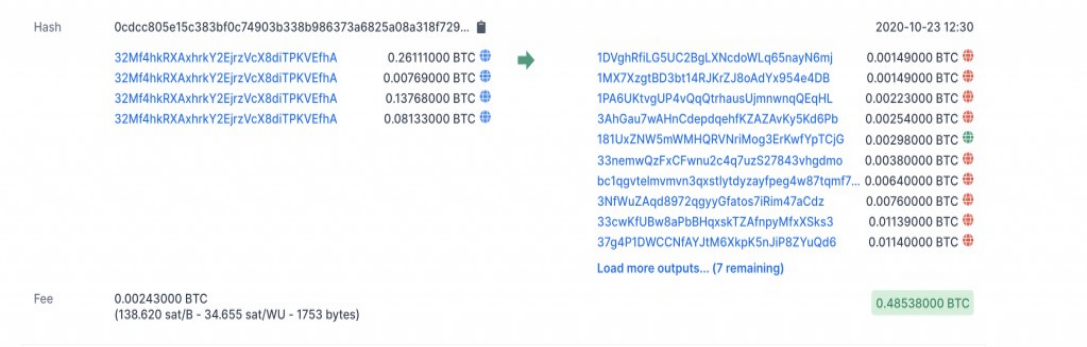
The irreversible nature of Bitcoin transactions are important for a whole host of legitimate purposes, but take notice of how these scammers want you to pay. No major investment corporation only accepts Bitcoin at the time of this writing. *None*. So be aware!



A suspicious Bitcoin-only deposit option

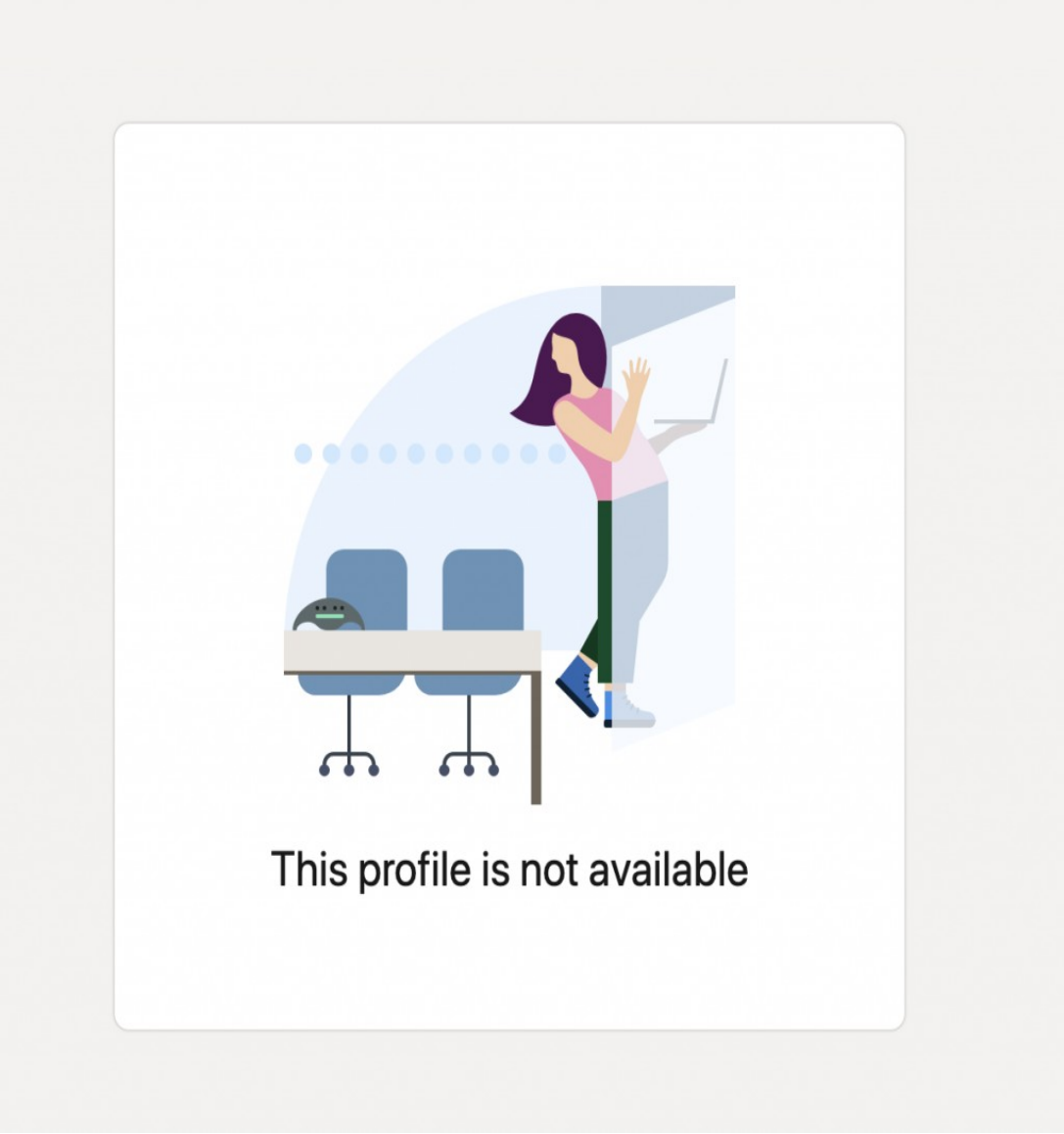
"Falling" for This Scam

It turns out, sadly, that some individuals did fall for this scam. When I checked the "deposit address" for my "investment account", I found that there were some existing transactions. So when my helpful associate from "Avior" asked for proof-of-deposit, I simply sent him a screenshot of an existing transaction



An unfortunate loss for a scam victim, and my fake proof-of-deposit

Once I sent my "proof" of deposit, lo and behold, my associate completely deleted his LinkedIn account thinking that he had run off with my money. Too bad for him, he was wrong!

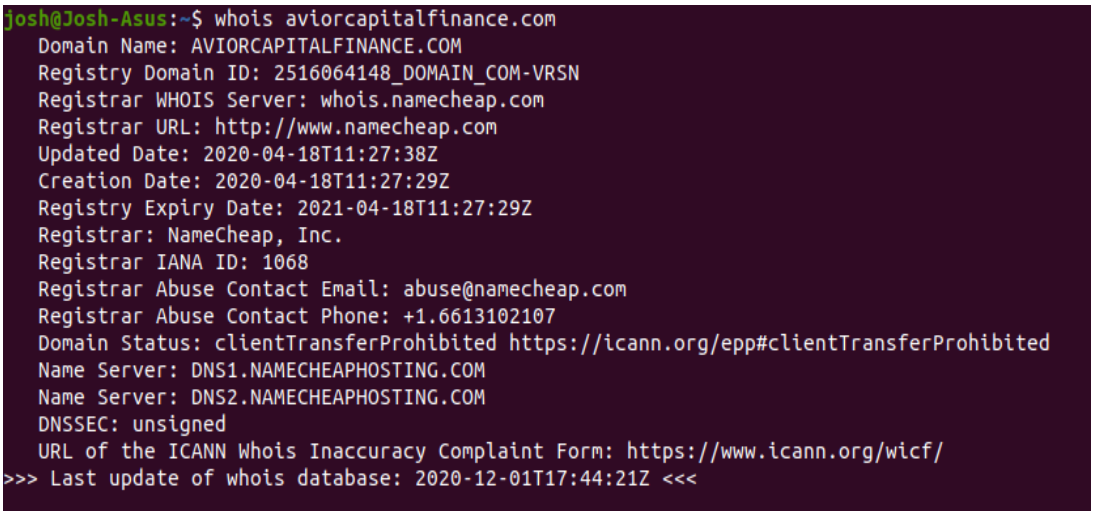


Social Engineering Scams - Be Aware!

No real money was lost in my case, and I had the chance to waste some of this thief's time. Not to mention, I got to make this fun and informative tutorial! This is just one example of a social engineering scam. Many variants exist, and these thieves use our human nature to prey on us.

Always double, triple check yourself when dealing with money - and especially with cryptocurrencies! The security features of the network can be used against you if you are not careful.

So what can be done about this? Well, in this case, I was able to see the public domain registration for the fake website via `whois`. I hope to report this scam website to their registrar, Namecheap, and get the site taken down.



Domain registration information for the scam website

In the meantime, be careful out there! It is best to *always hold your crypto yourself*. - Bitcoin is designed for you to hold your own money! Don't go chasing profits, and protect your own funds with a secure wallet.