

Cryptocurrency Impersonation Scams, Beware!

Author

josh

Date

2021-05-08 14:17:31

Overview

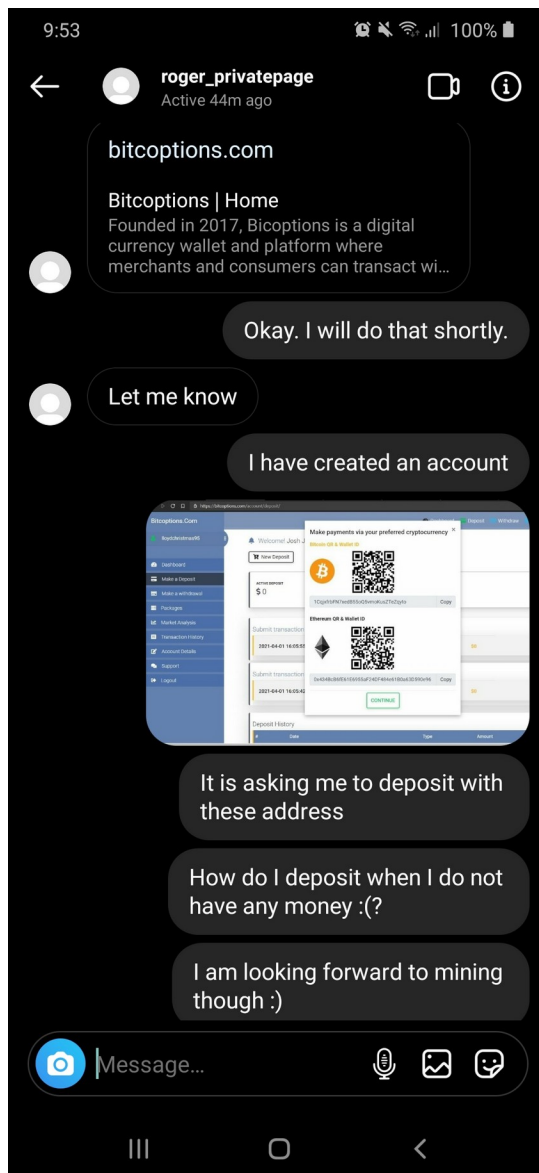
With the growth of cryptocurrency technology, scammers have found some rather innovative ways to separate Bitcoin from their rightful owners. Social engineering, the act of tricking a person into giving up keys or coins, is a common tactic. Humans are often much easier to hack than computer systems - so social engineering is at the forefront of the most common cryptocurrency related thefts. One of those social engineering tactics is *impersonation*, the act of pretending to be a high profile person or company in the cryptocurrency space in order to steal.

Types of Impersonation Scams

Investment Related Impersonation Scams

The first type of impersonation scam I often see is investment related. Investment scams are quite common in their own right, and the use of impersonation is an add-on way for social engineers to convince their victims that the "investment" they are offering is legitimate. In fact, the "investment" website or "account manager" is simply a scammer looking to take your money.

Scammers will impersonate high-profile individuals in the cryptocurrency space and cold-contact users, trying to get them to send them Bitcoin for an "investment opportunity" they are working on. For example, this fake Roger Ver contacted me and directed to a scam website.



Fake Roger Ver directs me to an investment scam website

Once the victim sends cryptocurrency, those coins now belong to the scammer with no way to reverse the payment. Part of the security model of Bitcoin is that transactions cannot be reversed once confirmed, so scammers use this to their advantage.


If someone contacts you claiming to be a famous person, or even a real life friend asking you to send cryptocurrency - *don't*. No legitimate investment opportunities require sending cryptocurrency to someone else. The whole point is that you get to hold your digital money!

Doubling Scams

Cryptocurrency doubling scams have been around for several years now, and a famous Twitter compromise led to several of these scams making headlines. The doubling scam uses impersonation to lure victims with a "generous" giveaway opportunity. A wealthy person or

company is usually impersonated, directing to a website or Youtube "livestream" where victims are asked to send some amount of cryptocurrency to "verify" their account and receive double their money back. For example: send 1 BTC to receive 2 BTC back.

This is *always* a scam. The only thing someone needs to send you cryptocurrency is your *public address*. You never have to send anyone any amount of crypto to *receive* money, you only need to give them an address. That's one of the things that makes cryptocurrencies so useful!



CHAMATH PALIHAPITIYA
5,000 BTC GIVEAWAY

More info on chamath-btc.org

2020

Use the QR Code or BTC Address to join:
● 1ZHiY6fQFiMgGyAfFBKDd324LUr5bf8ss

To participate, you just need to send 0.1 BTC to 20 BTC to the contribution address and we will immediately send you back 0.2 BTC to 40 BTC to the address you sent it from.

If you send 0.1+ BTC, you will receive 0.2+ BTC back
If you send 0.5+ BTC, you will receive 1+ BTC back
If you send 2.5+ BTC, you will receive 5+ BTC back
If you send 5+ BTC, you will receive 10+ BTC back
If you send 10+ BTC, you will receive 20+ BTC back
If you send 20+ BTC, you will receive 40+ BTC back

You can only participate once.

bitcoin

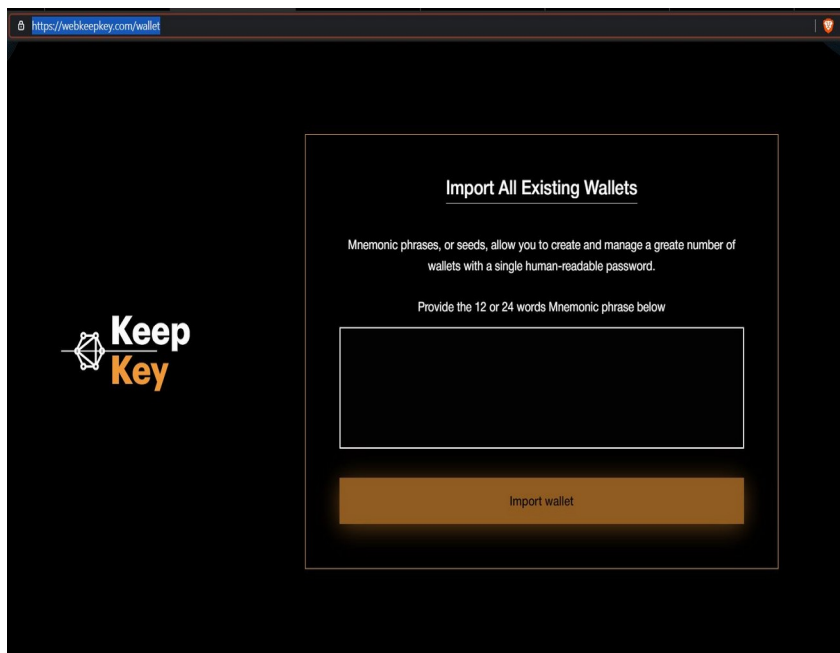
Watch NBC News NOW Live - Chamath Palihapitiya Live
54,752 watching now • Started streaming 58 minutes ago

2.3K 48 SHARE SAVE ...

A fake doubling scam

Recovery and Support Scams

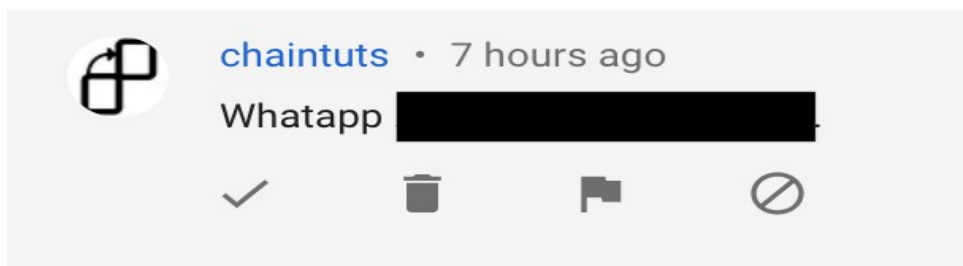
The final type of impersonation scam is often the hardest to spot, and also often the most damaging for victims. In this type of scam, the attacker impersonates the support service for a legitimate company or wallet, such as Coinbase, Blockchain.com, or KeepKey. They will masquerade as support, looking for victims that need help with their wallets or accounts. For example, this fake KeepKey "watch wallet" asks for private information you should *never* type into a website - your seed phrase:



A KeepKey phishing website

No legitimate wallet support will *ever* ask for your seed phrase, 2 factor authentication codes, or password. This information is always private.

Another form of impersonation scams is pretending to be a person in the cryptocurrency space endorsing a *fake* recovery service or wallet support. Given the prominence of scams and the irreversible nature of cryptocurrencies, many individuals are looking for recovery help when it is not even possible. Scammers prey on those victims to extract even more money from them. Here is a chaintuts impersonator directing people to a WhatsApp number:



A chaintuts imposter

These sorts of scams make my blood boil. I will never ask you to invest in anything, and discourage the sharing of seed phrases for recovery work.

Impersonation Scams - Be Wary

Anyone can pretend to be anyone on the internet, that is a fact. Be cautious about "Coinbase" asking for Bitcoin for a giveaway, and don't believe that "chaintuts" contacted you with a smart "investment opportunity". Social engineers are professional predators that use their skills to steal Bitcoin from people, and it is an unfortunately lucrative criminal enterprise.

Never send someone cryptocurrency with the promise of too-good-to-be-true returns. Don't ever give anyone your seed phrase or 2FA codes. Above all, be cautious. Being your own bank is a great thing, but it comes with more responsibility than a checking account does. Go slow, ask questions, learn lots, and stay safe!