How Bitcoin "Recovery" Scammers Operate

Author	josh
Date	2020-05-19 15:45:25

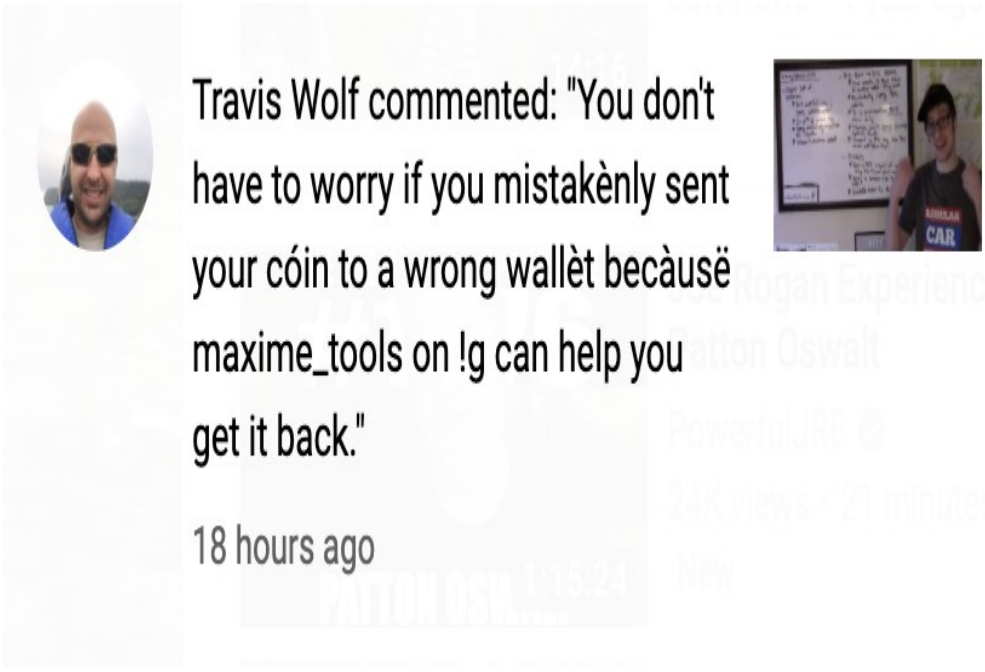
Overview

Sometimes, people lose Bitcoin. It is an unfortunate problem of a system that is very secure and has irreversible transactions by design. Sometimes, it is possible to recover lost coins. There are legitimate services out there than can help in the event of lost crypto, but many more that are scams that prey on users to steal *even more* coins.

How Recovery Scammers Operate

Spam Advertising

I was inspired to create this tutorial due to the annoying volume of spam comments I get on the chaintuts YouTube channel. They often look something like this:

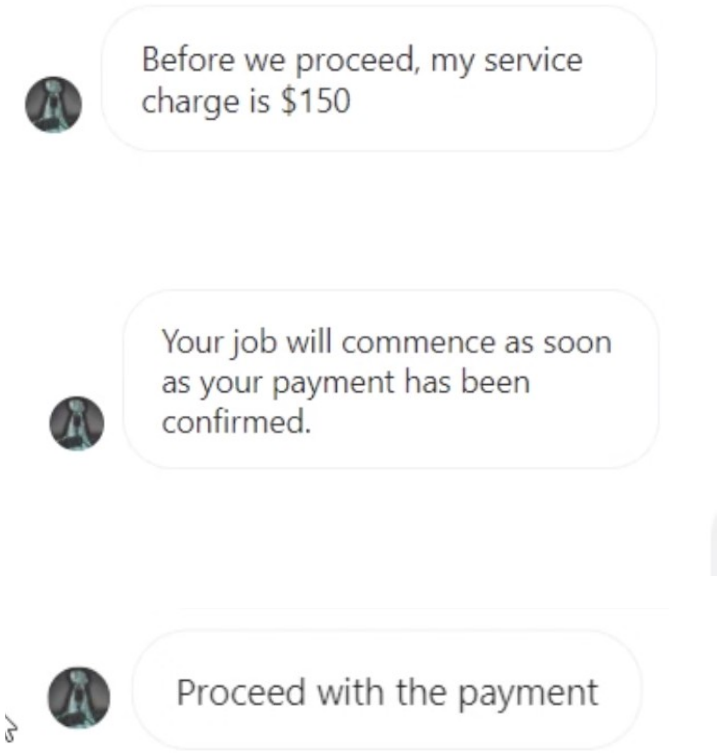


These scammers likely pay for fake account bots to post these all over relevant videos. I see these most commonly on my more popular videos that discuss legitimate coin recovery steps. I quickly delete them, and many times the YT spam filter catches them before they get to you. But alas, some people will inevitably see these and perhaps contact the scammers.

What Do They Try and Get From You?

So what do these individuals want from you? Well, they certainly want your coins. But how do they actually try and get them?

The first way in which they steal from you is simple: they demand payment up front. Legitimate coin recovery specialists or crypto experts that will try and help you usually only charge a percentage of whatever is recovered. These folks though? They want money up front:

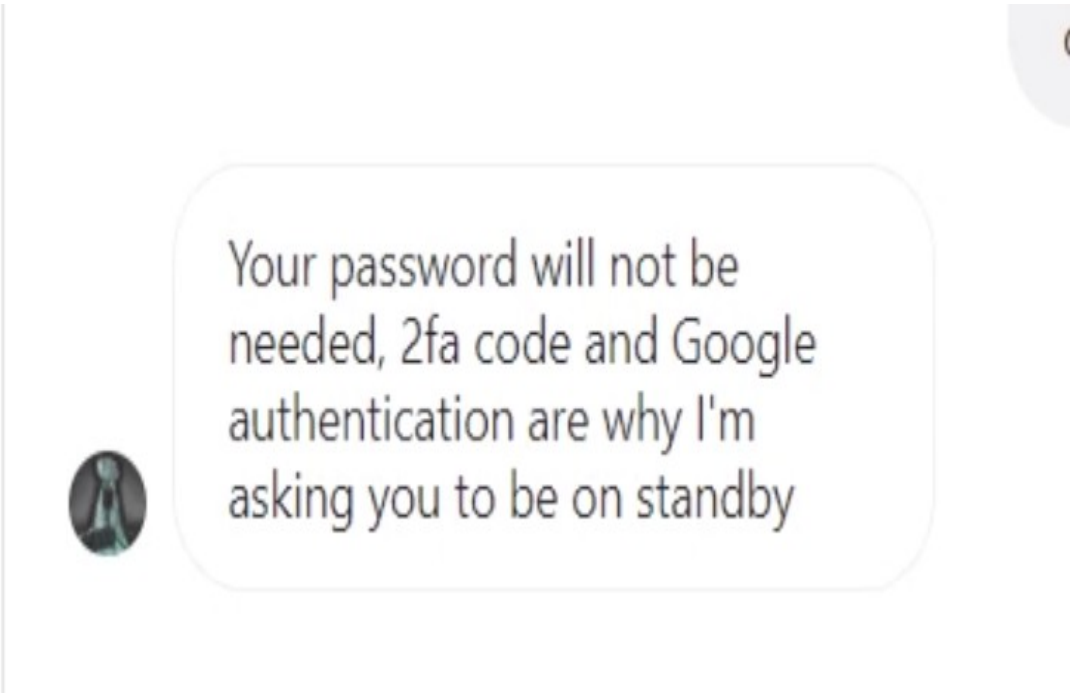


This individual is very insistent that they be paid first. So one possible method of scamming their victims is to simply take their charge in BTC and ghost you. Transactions are irreversible so there's nothing you can do once you pay them.

But it doesn't stop their. They want access to your online accounts such as online wallets and exchanges, using a slightly devious tactic...password resets with your help.

In order to get into your account, they won't ask for your password. They will, however, ask for your email and ask you to "be on standby" to give your two factor authentication codes.

This might seem a little better to an unsuspecting, desperate crypto newcomer. You're not giving away your password, right? However, one should NEVER EVER give away 2FA codes. They are for you and you only. The scammer will initiate a password reset on your account, verify they are "you" by taking your 2FA code, and then accessing your account.



This is a type of *social engineering* attack. They're not "hacking" anything technologically speaking, but are tricking you into willingly giving them sensitive account information.

With your pre-paid (stolen) BTC and access to your online wallets, thieves can potentially steal thousands of dollars worth of crypto from you.

Avoiding Social Engineering Attacks

First, I would never prepay for recovery service. Most crypto folks will be willing to help you out some for a percentage of the recovered funds. Secondly, never give out sensitive account information such as passwords or 2 factor authentication codes. These can be used to steal your accounts and lock you out from them permanently.

Lastly, we should talk about seed phrases. As a general rule, you should *NEVER, EVER, EVER give out your seed phrase.* Your seed phrase (12-24 words given to you by your wallet) gives access to ALL of the coins in that wallet. So someone can use it to steal all of your money.

The only case in which you may consider doing so is if you are working with someone you trust, and if you remove your other coins and *no longer use that phrase, ever.* Individuals sometimes reach out to me for help with coin recovery, and if it's possible in that case a seed phrase is required to try and find the right private key for coin recovery. However, I try to walk users through the steps themselves without getting the seed phrase at all, and only accept seed phrases for recovery if the user wants me to do it for them. In that case, I always recommend "burning" that phrase after recovery.

It's up to you to keep your coins safe, so don't give away your personal information!

Don't Use These Fake Services

It goes without saying, but still, don't use these fake services! If someone is spamming YouTube comments about their amazing hAcKeR rEcoVerY SeRviCes, then chances are pretty good you can't trust them. Instead, reach out to a trusted crypto-savvy friend if you make a mistake. Stay safe!