You can now subscribe to get stories delivered directly to your inbox.

Got it

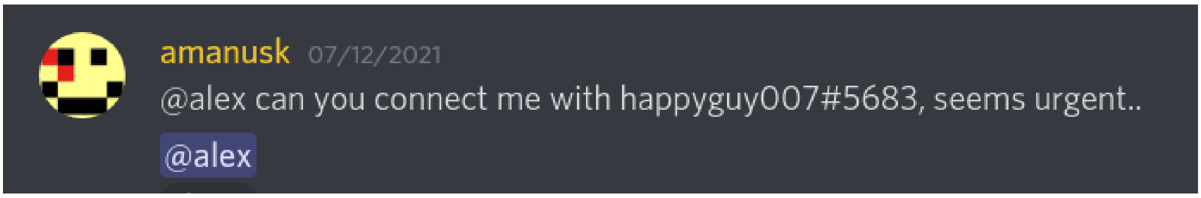
Frontrunning a Scammer

Alex Manuskin Jul 16 · 14 min read

A rather regular afternoon was interrupted by a message in the flashbots discord. I sometimes check out messages there and see if someone needs help recovering funds. This time the message seemed quite urgent. The victim was losing tens of thousands of dollars by the minute. What followed was an 8-hour hackathon to try and save as much of it as possible.

The user u/happyguy007 wrote a detailed and excellent account, documenting in real-time how it feels to fall for a phishing scam.

This is the story of what it looks like from the other side. Before we begin, here's a short introduction on how to get phished.

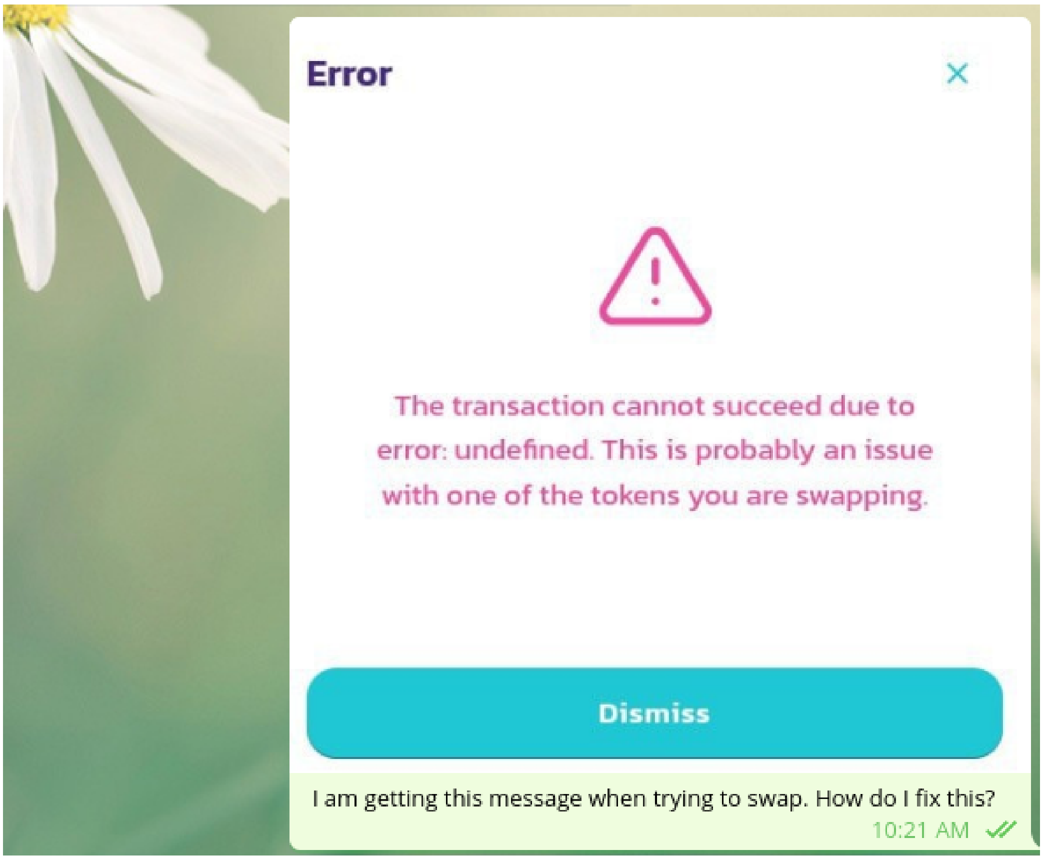


amanusk 07/12/2021
@alex can you connect me with happyguy007#5683, seems urgent..
@alex

How to get scammed

If you would like to experience getting scammed by phishing sites firsthand, here is how you would go about it.

Go to any public server of a known project, (e.g. Discord or Telegram), and ask basically any question where you request help with locked funds or a stuck transaction. Sketchy projects attract many scammers (if you want to improve your chances), as they often lurk in chats with high levels of FOMO. Telegram is much worse than discord in that regard, as it is much harder to organize and moderate.



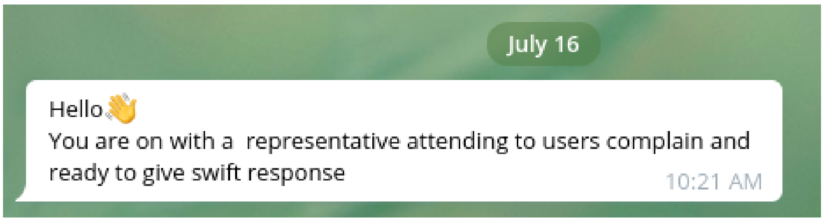
Error

The transaction cannot succeed due to error: undefined. This is probably an issue with one of the tokens you are swapping.

I am getting this message when trying to swap. How do I fix this?
10:21 AM

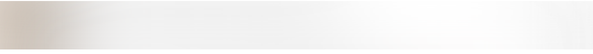
Innocent request for help

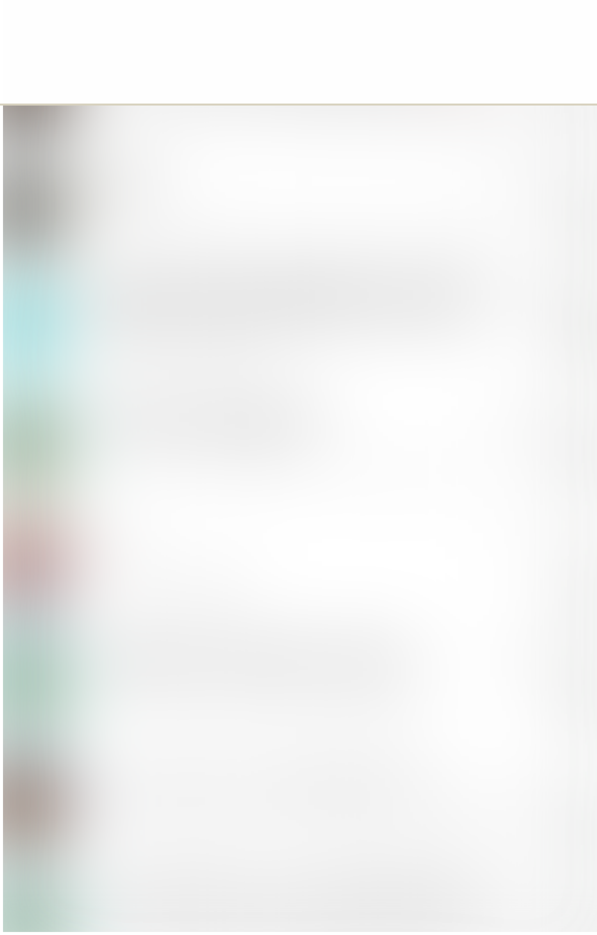
Within minutes of asking a question an army of “tech supporters” will flok into your DMs offering help. Not sure how it works behind the scenes, but it seems there are actual farms of these scammers, employing personal to lurk and respond to these messages



July 16

Hello👋
You are on with a representative attending to users complain and ready to give swift response
10:21 AM





Everyone and their bunny wants to help you!

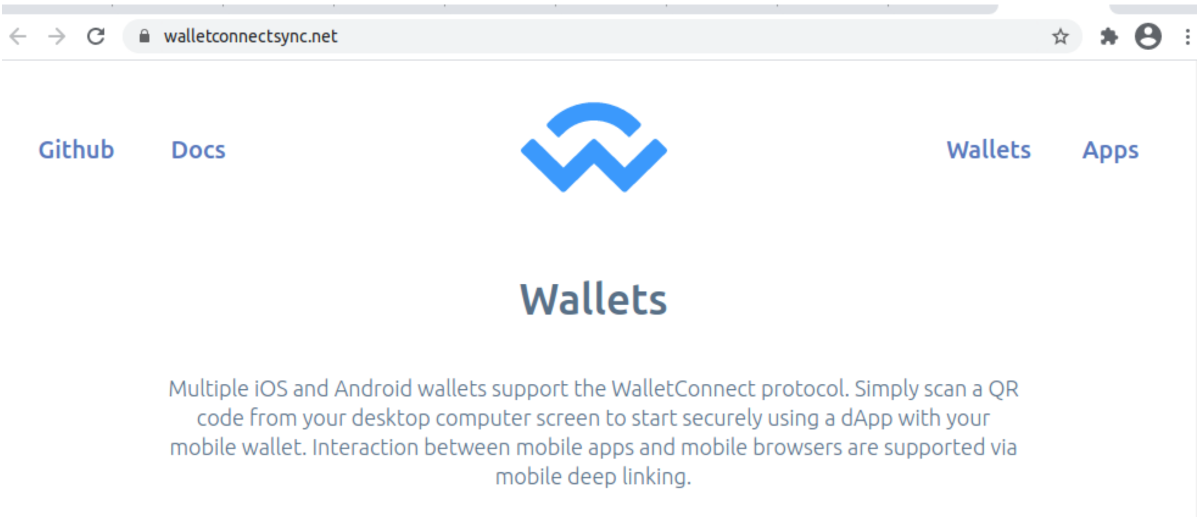
Some of them are even smart enough to request that you delete the original message asking for help from the public chat. They know that there are dozens of other lurkers springing into action at once, and they don't want anyone else to be able to "help" you.

The tech supporter will usually ask a few questions, "describe the problem", "what wallet are you using" etc.

Regardless of what the issue is, the answer is always the same. "There is some problem in the database, and you have to sync your wallet".

Of courses, there is no database, and there is no need to sync any wallets (this is what the blockchain is for). The truth is, dAPPs have bugs, and bugs have people asking questions, and people who are eager to not waste the opportunity to make 5000% APY before the rug pull, or who have just sent $10K to some farm and don't immediately see the balance reflected, will naturally be concerned and want to talk to someone. This is the scammer's bread and butter.

The representative will then (kindly, it's always kindly) provide a link to a website that usually looks like a MetaMask or WalletConnect clone. The website URL will be some legitimate-looking word combination of "wallet" and "connect". The website will have SSL encryption (easy with letsencrypt), and if you ask about it, they will assure you that everything is end-to-end encrypted and safe (lol). There are infinite domains they can use for the same scam and cycle through them every time one gets flagged or shut down.

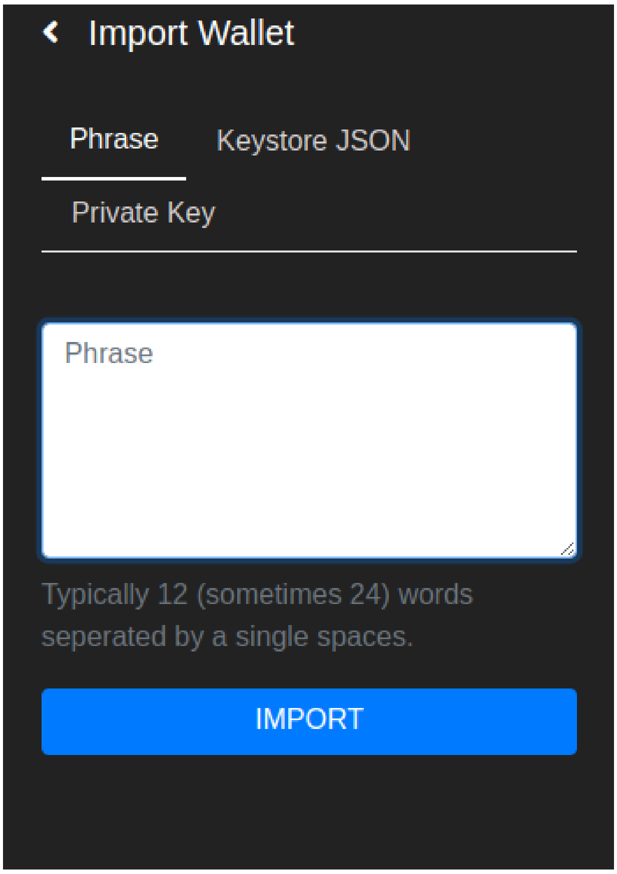


Wallets

Multiple iOS and Android wallets support the WalletConnect protocol. Simply scan a QR code from your desktop computer screen to start securely using a dApp with your mobile wallet. Interaction between mobile apps and mobile browsers are supported via mobile deep linking.

Example of a phishing site impersonating WalletConnect

The website will have links to all the popular crypto wallets. No matter what wallet you use, or which one you click, you will get a page where you are requested to paste either a seed phrase or the private key (they give you options!)



Import Wallet

Phrase

Keystore JSON

Private Key

Phrase

Typically 12 (sometimes 24) words seperated by a single spaces.

IMPORT

Example of a phishing site requesting a seed phrase

Once you do that, the game is over.

At this point, nothing will really happen. No problem or issue will be resolved, and the representative will disappear or keep you engaged while they empty your wallet.

Sooner or later, it might dawn on you that this is exactly what they tell you not to do. NEVER GIVE YOUR SEED PHRASE OR PRIVATE KEY TO ANYONE.

But again, it is too late.

Here is a list of things that won't help:

- Unlinking your wallet from the dAPP
- Logging out of your wallet
- Changing the wallet’s password
- Deleting your wallet and burning your PC/Phone

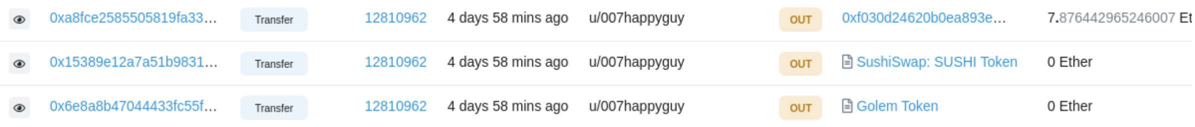
The seed phrase is the private key to your account. If you give it away, it’s not yours anymore. Whoever has it can connect from any other wallet, from any other computer, and from anywhere in the world.

Back to our story

The experience of happyguy was probably something similar. According to their own account, they were approached by an impersonator on the SNX discord server and gave away the private key.

Scammers come in different shapes and sizes. Unfortunately for happyguy, these were the slightly more sophisticated kind.

They immediately emptied the wallet from some tokens and almost all the ETH.



👁	0xa8fce2585505819fa33…	Transfer	12810962	4 days 58 mins ago	u/007happyguy	OUT	0xf030d24620b0ea893e…	7.876442965246007 Et
👁	0x15389e12a7a51b9831…	Transfer	12810962	4 days 58 mins ago	u/007happyguy	OUT	SushiSwap: SUSHI Token	0 Ether
👁	0x6e8a8b47044433fc55f…	Transfer	12810962	4 days 58 mins ago	u/007happyguy	OUT	Golem Token	0 Ether

Transactions outgoing to the scammer’s wallet

These transactions were executed within a single block, suggesting the scammers had some automated script in place to grab as much as possible. They were also smart enough to use a fresh Ethereum address, as they didn’t need to get ETH from anywhere else. They had all the ETH they needed for gas from the compromised account. (Destination addresses of the scammers: address1, address2)

After the initial sweep, the scammers returned to the crime scene to pick up the pieces.

Why didn’t they empty the entire wallet on the first block? Fortunately for happyguy, not all funds in his account were just ERC20 tokens and ETH. Some tokens were less well known (e.g. LP tokens) and some were locked up or staked in various protocols. These are the funds that might still be saved.

A punching fight

Reading the blockchain, it seems the scammers and happyguy himself were exchanging blows. The scammers sent some ETH back to the account, with the intention to begin withdrawing funds from other protocols where funds were locked up. They were quite successful at that.

a script, happyguy was losing out in most battles. The scammers were successfully removing tokens from the account and leaving no ETH for happyguy to do anything about it.

Making any transaction such as sending out ETH or tokens is much harder to perform manually by simply pointing and clicking. If the scammers were indeed running a bot, it would be impossible to beat them manually.

Happyguy was able to remove some of the ETH and tokens, but most were going to the scammers. Trying to send ETH to the account and salvage some tokens would just cause more damage. The scammers used the received ETH to remove the tokens themselves. All hope seemed lost.

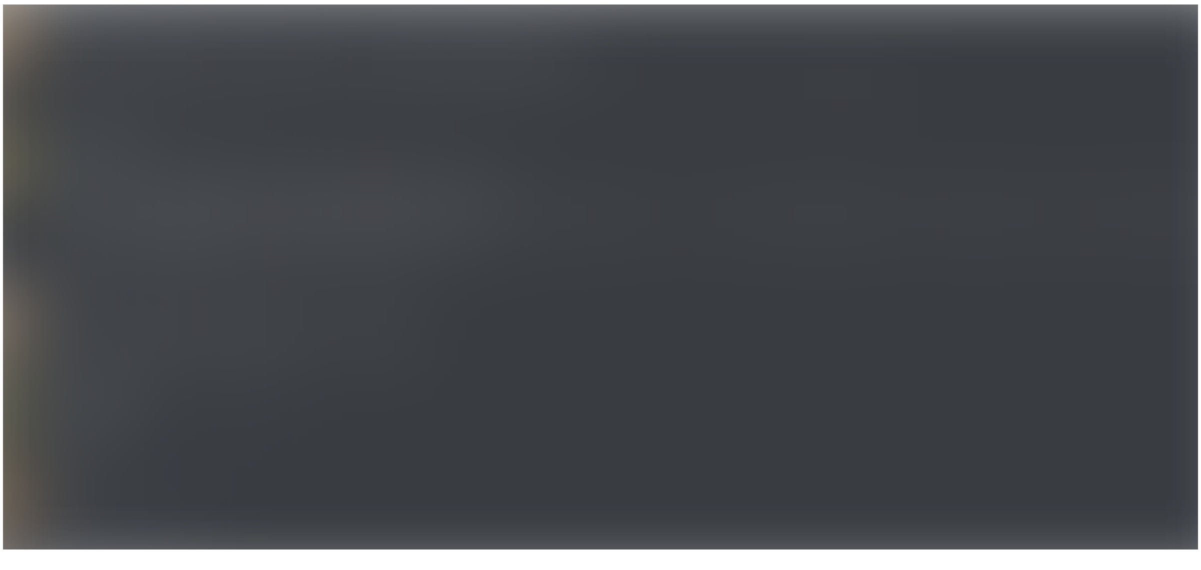
Serendipity

About 6 hours after the account got compromised, word of the event had reached the flashbots discord. It usually takes some time to go over the details of the case before anything can be done about it, but this case seemed urgent.

As someone who had a chance to do this a few times, it is important to make sure that the account owner is indeed who they say they are. There were cases before where several people claimed ownership of the same account.

This usually happens because another popular scam is to try and sell compromised private keys on the “second-hand” market. These scammers try to sell an account that has already been compromised. The account might have some tokens, but ETH must be sent to it to move them out. The scammers then scoop up any incoming ETH for an easy profit. (example).

Some “victims” show up asking to replicate this behavior so they could profit themselves (rule of thumb, don’t engage with people you don’t know who call you “bro”)



To validate the ownership of an account one can ask the owner to sign a message from an account they have access to. Naturally, it cannot be a message from the same account, as this could easily be the scammers.

A decent approach is to find another address with which the account interacted. Obviously, it should be an address they have interacted with before they got phished, and the earlier the better. This service of MyCrypto can be used to sign and verify messages without paying for gas.

Once the account is verified — the tricky part starts. Having access to the account requires the private key. The number one rule (and the reason that this happens at all) is to never give anyone your private key or secret seed phrase.

There is no easy way around this. The scammers have access to the account and can reign rampage and do whatever they want. Getting the same level of access might be necessary, especially if time is of the essence, as was the case here. This time it was necessary for happyguy to share the private key (again), to have any chance of fighting back.

Fighting back

Once the private key is received, the first order of business is to stop the bleeding. This is done by running a “burner” script on the account, which does its best to remove all incoming ETH to the account.

ETH is necessary to perform any operation on the network. It is used to pay the miner fees. Removing any ETH makes it a much harder job for the scammer to keep performing operations and emptying the account from tokens or interacting with protocols.

The burner was set up, and after a minute it had received the first payment from the scammers, looking to empty some additional tokens from the account.

Burning hurts

The burner works in a simple way. If ETH is detected in the account, try to spend as much as possible as a fee to the miner, and send the leftovers to some unrelated address. After the scammers’ deposit, all funds are paid to the miner, and the remainder is sent to the burn4Ever address (everyone will all be richer soon ;)). The burn Tx in this case paid 3000 Gwei to the miner, way above the average gas price at the time.

What makes the burner effective, is the fact that it uses the entire ETH balance of the account to pay a fee to the miner.

given amount of ETH in the account, an Ethereum transfer would pay the most per unit of gas, making it more preferable to the miner.

But what if the scammers run a script and broadcast their transaction super fast? Here's where another important feature comes in. An Ethereum transaction can be replaced after the broadcast, as long as they have the same nonce, and pay at least 10% more for gas than the transaction they are replacing.

Since any valuable transaction of the scammers would likely require more than 21000 gas, it can be outbid by paying ALL the balance to the miners and sending the most basic transaction possible. As long as a burn transaction is sent, it is most likely to override and replace any transaction initiated by the scammer

Running the burner thus makes it quite hard for the scammers to make any transaction originating from the compromised account. Even if they run a script to steal the funds, their transaction would be front-run by the replacement burning transaction.

Back door extraction

Once the bleeding was stopped, it was time to try and extract what was still salvageable from the account. It is important to note here that whoever has the private key, has the same level of access to the account. It is not possible to make any remote operations that will hinder the scammer's capability. So anything a white hat can do, the scammers can do. Success is not guaranteed.

It thus becomes a race of who can extract the most, the fastest.

So how does one extract funds from an account where any ETH sent to it is burned? This is where flashbots come in.

Flashbots is a service that enables sending transactions directly to miners (via a relay). Importantly, it allows the creation of bundles of several transactions that can be executed atomically (sort of).
Normally, a transaction is the atomic unit on the Ethereum blockchain. A transaction can either succeed or revert. A reverted transaction does not change the state (but does

ETH to cover the gas costs. This is exactly why the burner is so effective.

A bundle, however, can ensure a miner that they will be paid (generously) if and only if they execute a series of transactions exactly in the order you requested.

Let's look at an example.

Funds are staked in a protocol. To remove them, we would like to remove them from the stake protocol and send the funds to a safe address, without giving the scammers a chance to remove the tokens.

An extraction bundle would look like this:

1. Unstake the funds
2. Transfer tokens to a safe address
3. Pay the miner

Steps 1 and 2 can be done with 0 gas paid to miners. In step 3, a contract call can be put in place, which checks a condition. If the condition is met, the miner gets paid. The appropriate condition, in this case, could be: "make sure the **safe** address has exactly X amount of tokens at the end of the bundle".

The bundle is sent directly to the miners via the flashbots relay and is only executed if all transactions take place.

Real-life example from the happyguy case:

1. Withdraw
2. Transfer
3. Pay

Notice that all three steps pay 0 gasPrice, and the last transaction has a direct payment to the miner.

Direct payment to the miner

The fact that transactions in the bundle are private is a nice feature, but it is not what makes this work. When building a bundle, consider the fact that transactions might

once.
Block space is quite valuable to waste on a non-paying transaction. The last transaction that actually makes the payment can only take place if the previous transactions were included before it. This creates (but does not guarantee) an atomic bundle to extract funds.

Here comes the cavalry

Although we were ahead and had some tricks up our sleeve, the fight had just begun. As stated, the scammers have the exact same access to the account as we had, so there was still a question of being better than them.

The plan was to start removing funds from the most to the least valuable protocols, starting with some funds locked in Curve stETH pool. Most remaining funds were in that pool (~40ETH), and it was slightly trickier to make the extraction.

Removing ETH from a protocol might be dangerous. Considering the burner script was running, if raw ETH would end up in the account, 40 ETH would have immediately been paid to the miner as a fee. Fortunately, in this case, removing the deposit as stETH is also possible, and thus preferred.

The pressure was on to write the extraction script as fast as possible before the scammers figured out what was going on. The fact that the scammers were actively sending funds to the account created some stress. The burner script is a good trick, but it might still fall short if there is some communication error and the incoming transaction is not picked up fast enough.

Furthermore, this was quite a lot of money. In many of these cases, there is no real-time pressure, the accounts might be long forgotten, or have funds locked in a way that is not immediately accessible. In this case, the scammers knew and were actively trying to remove the funds as well.

So time was of the essence, but a lot was at risk. Having ~$80K of someone else's money on the line, depending on some script hacked in a half-hour is rather stressful, so you do what you can to make sure it will work.

Before sending the actual bundle, it is possible to simulate it to get an idea of the results and debug it. Once the simulation works as expected the bundle can be created and relayed to flashbots.

Luckily, the script did work. The funds were successfully transferred to a safe address, and we could continue to the next protocol. (Looking back, it was probably safer and easier to just move the CRV LP tokens)

Scammers might have noticed the activity on the account and tried sending in some more ETH. It was successfully burned as well.

Knowing the burner is holding its ground, and the bulk of the funds were safe, we could continue to recover the rest of the funds.

Overall we recovered funds from Curve, Sushi, Alchemix, Uniswap, Balancer, and others. Each requires a slightly different approach and some research.

Epilogue

After most of the funds were recovered, I discovered the entire process was "streamed" by Happyguy on a Reddit post. Perhaps some of the comments led them to the flashbots discord, where we could help. It was quite an intense few hours, working on recovering as much as we could. About ½ was lost, and ½ was recovered. Still a costly mistake

How to avoid falling for a phishing scam

Many comments on the Reddit post scoff at the fact that the private key was compromised. Obviously, you should never give away the private key or seed. But this can happen to anyone. We had witnessed multiple cases, from first-time users and long veterans.

Protocols and UIs can be confusing, and the scammers are there to feed off the user's pain. Here are some best practices to avoid ending up in the flashobots discord (although you should definitely join).

1. DON'T PASTE YOUR SECRET SEED INTO ANYTHING ONLINE. It's been said a million times, but still worth repeating
2. Use a hardware wallet. The keys are stored on the hardware wallet, so you should never even experience typing or pasting them onto a laptop/phone. The very

don’t do it.

3. Diversify your holdings. Having all the eggs in one basket is dangerous. Consider spreading it around between several accounts, and even several protocols. In this case, it helped slow the scammers down
4. Use different wallets. Some wallets such as ZenGo, Argent, and Gnosis do not use a seed phrase at all. Using less ubiquitous solutions makes it more difficult for scammers to attack.

If you do find yourself in the same situation as happyguy, reach out to the flashbots discord.

Finally, providing this help would not have been possible without Alex, Scott, Santiago, and others from the flashbots crew.

Also thanks to Maor for the help writing and reviewing this post.

If you would like to donate gas money for future extractions, you can send some ETH here:
0xf3544bc8b85ead19352183c9f1f0a592634cb9c3

Stay safe out there

Twitter: @amanusk_ | Github: @amanusk

Ethereum Flashbots Phishing Scam Security

Get the Medium app

Download on the App Store

GET IT ON Google Play