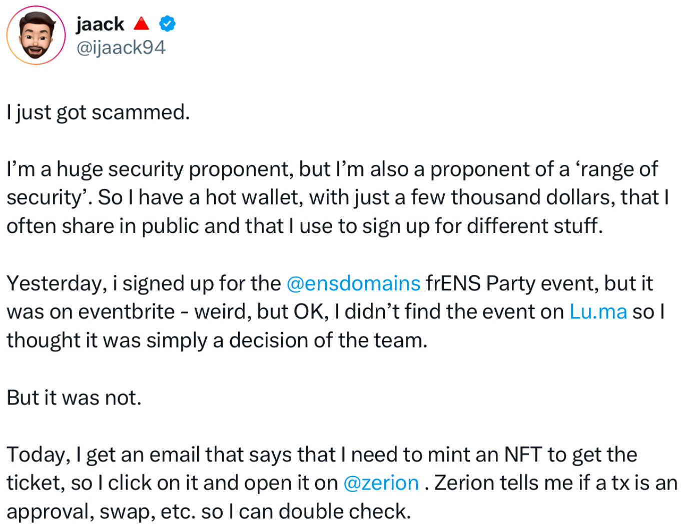
My main hot wallet got compromised. Here's what I learned

I've had the same hot wallet for years. Specifically, for more than 7 years, since I joined crypto and I set up my first non-custodial wallet on Exodus, the first multichain wallet that was out there back in 2017.

Though I have other (many) other wallets in cold storage, this one was the one I used the most for various reasons:

- It was convenient, because I didn't need to sign every transaction with my PIN like I do on my cold storage
- It was akin to my identity, and many platforms actually **incentivize users to have one single wallet** to evaluate onchain metrics like onchain activity and such
- It was the first, so even though I had other hot wallets, I always used this one because I didn't have to switch when in my browser or mobile wallet.
- After joining avascan / routescan, I used it to make transactions when debugging our products across all the chains we support



jaack
@ijaack94

I just got scammed.

I'm a huge security proponent, but I'm also a proponent of a 'range of security'. So I have a hot wallet, with just a few thousand dollars, that I often share in public and that I use to sign up for different stuff.

Yesterday, i signed up for the @ensdomains frENS Party event, but it was on eventbrite - weird, but OK, I didn't find the event on Lu.ma so I thought it was simply a decision of the team.

But it was not.

Today, I get an email that says that I need to mint an NFT to get the ticket, so I click on it and open it on @zerion . Zerion tells me if a tx is an approval, swap, etc. so I can double check.

I will not dive into details on how it got compromised, but let's just say that I first got phished after signing up into a DEVCON side event, then I got scammed by someone impersonating someone else that could have helped me. In the first case, I could have been more careful, but I was so stressed in those hours that I should've predicted that something like this could happen.
In the second case, I really wouldn't blame myself because I was completely out of my mind, I was afraid because I realized that I got phished immediately, and I didn't know what the exploiter had access to, so I trusted the wrong guy.

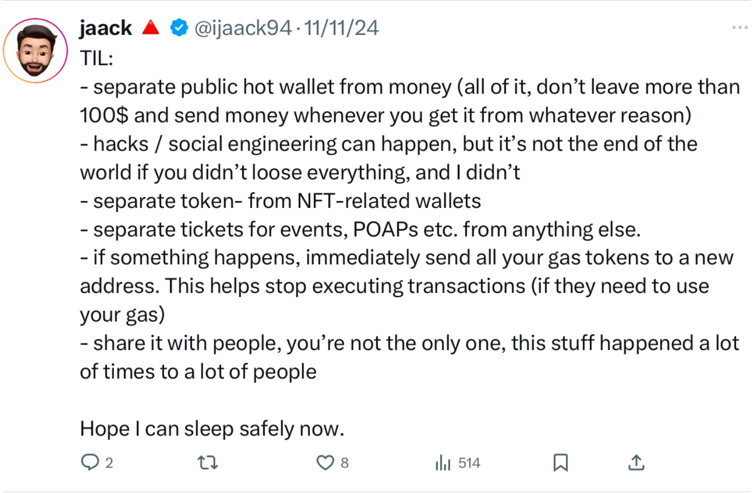
I lost 90% of my holdings in that wallet, but I still could save some things that were important to me, and here is where I want to make a case:

A wallet is increasingly becoming an online identity, beyond onchain even.

In that wallet, I had *all my onchain identities:* my ENS, Blast domain, Avvy domain, all the articles I had saved on Mirror. I recovered everything because nor the exploiter neither the scammer saw value in those (luckily), but this made me really aware of the risks users take when they decide to have "one wallet = every dapp".

This paradigm was a necessity in 2017-2020, when embedded and smart wallets were not out for the public. But now that we have all this tech

available to fragment our identity, I appreciate it.



jaack ▲ @ijaack94 · 11/11/24

TIL:
- separate public hot wallet from money (all of it, don't leave more than 100$ and send money whenever you get it from whatever reason)
- hacks / social engineering can happen, but it's not the end of the world if you didn't loose everything, and I didn't
- separate token- from NFT-related wallets
- separate tickets for events, POAPs etc. from anything else.
- if something happens, immediately send all your gas tokens to a new address. This helps stop executing transactions (if they need to use your gas)
- share it with people, you're not the only one, this stuff happened a lot of times to a lot of people

Hope I can sleep safely now.

For this reason, I started creating other wallets, one for each general purpose (tokens, NFTs, identity) and then start preferring non-custodial, embedded wallets or smart wallets for each app as opposed to one wallet for everything.

A couple of years ago I would've gone crazy managing all these EOAs, but now it's all very much simple. I created my Zora embedded wallet for NFTs for example, and every time that I see that that wallet has some valuable NFTs I don't want to lose, I send them to my cold storage. I now check this, because I didn't do it before.

And also, the Trump election while I was flying to Bangkok for DEVCON didn't help either. In fact, I had many coins that were worth tens of dollars, and in a few days got worth hundreds, because of the pump. To me, I didn't lose the 10,000$ or so that was worth in that wallet at the time I got phished, but much less, some 5-6k, because that was my perception of the worth of that wallet.

It got frozen, in the chaos of DEVCON in Bangkok.

And the money, believe me, wasn't the issue - I wasn't worried about the money, but as I said, about the onchain identity. And the affection / love for what it was there, all the memories associated with NFTs I minted, coins I bought that then rugged (I still got a very tiny fraction of Snowdog to remember the wild bull run of 2021!), and everything else in between.

It held my story, and now that wallet is gone. Not just mine anymore. Mixed with someone else's history of theft.

——————

Security is a spectrum, so I won't go and close everything I do and put everything in cold storage just because I had this happening to me.
First, it's the first time this happened to me in **more than seven years** of being onchain and doing tens of thousands of transactions, so it's kind of okay if you think about it. For the volume of transactions I had, it could have been worse. And that's because I'm always very careful, and this would surely not have happened if I was at home, simply because I get many phishing and scam attacks every day via email or on X, and I never fall for them. But I was in a very fragile state of mind in that moment.

So of course I have increased my security requirements, but I have not made them so hard to apply that they're forcing me to do nothing. They're there to help me be safe as much as I can.

And that what I'll do going forward.

Date: 2024-12-10
Words: 868
Time to read: 4 mins

Newer Older

5th February 2025
Shutting down mantlescan.info

29th September 2024
High-throughput chains with lo...

Tags Archive RSS feed Twitter Instagram GitHub Email QR Code

Made with Montaigne and bigmission 🇺🇦