

Forum:[Hack Forums](#)

Thread: [ALERT: Anyone using Blockchain.info](#)

Regular Guy - January 1, 2015, 2:11 am

So, this is the second time this has happened to me but today, one of my many blockchain.info wallets was hacked.

Now, this wallet was NOT mine, it was a shared wallet with a long time partner of mine who had majority of his BTC in it as well as a small portion of my own.

MY wallet had:

- 2auth
 - Secondary Password
 - IP logging (in case of suspicious activity)
 - a 13char password including caps, numbers and special characters
- My wallet was prepared for this sort of attack, as this has happened to me with a 20BTC amount in June 2013 when the value was a little lower.

On the other hand his wallet had:

- 2auth
- NO secondary pass
- NO IP logging
- A weak-ish password

For the record, my WALLET WAS NOT compromised but I am here to let you know that 2auth accounts CAN be compromised!! Our Private Keys were NOT public, nor were they ever shared on an opensource/logged chat room. All were encrypted via PGP messages so it would not have been a security leak.

Blockchain Hackers have been around for ages and surprisingly blockchain has done jack shit about it...This is just to let you know that even small wallets with .1BTC can be hacked.

We lost 3BTC in this hack, I won't reveal the address due to my own security but it's a considerable loss. I hope you ALL keep your wallets safe with not only 2auth but EXTREMELY strong passwords and secondary passwords. NEVER hint your password to anyone. Blockchain.info is easily bruteforce-able, so if you have a weak-ish password, UPDATE it to a 10+char (the more the better) password IMMEDIATELY, or simply get rid of the risk and use an online wallet.

Why did I use blockchain instead of offline wallets like I CONSTANTLY endorse on this board? Convenience. I only ever use it for convenience, and today, the cost of convenience was not what I planned on paying vs' using an offline wallet.

Stay Safe

-Regular Guy

Sacred Symmetry - January 1, 2015, 2:14 am

Jesus, sorry to hear about this bro.
Shits getting outta hand

w34k - January 1, 2015, 2:17 am

(Jan 1, 2015 03:11 AM)Regular Guy Wrote: [\[CITE\]](#) I am here to let you know that 2auth accounts CAN be compromised!!

Yeah, old news to me. I always suggest using an offline wallet. Blockchain.info is sketchy. Although some prefer convenience over security. ?

LordCoder - January 1, 2015, 2:23 am

Trust me, having the Bitcoin-qt is the best thing you can do. Leave it syncing 3-4 days and you're ready to use it fully. Takes 2 mins to sync everyday and you're secured. Online wallet means you don't have ANYTHING. Think about it.

Autocorrect - January 1, 2015, 2:25 am

Why would you store so much BTC in a hot wallet?

Figma - January 1, 2015, 2:25 am

That's exactly why you should use Coinbase instead of blockfail.

Speaker??? Knockertz - January 1, 2015, 2:27 am

My password is like somewhere around 40-45 characters lol it takes me a while to get in.

Autocorrect - January 1, 2015, 2:28 am

(Jan 1, 2015 03:27 AM)Childish Gambino™ Wrote: [\[CITE\]](#) My password is like somewhere around 40-45 characters lol it takes me a while to get in.

<https://lastpass.com/>

Makes long passwords a lot easier.

Encryption is mandatory if you're paranoid.

Moen - January 1, 2015, 2:30 am

I am sorry for your loss, Are you gonna limit your use of blockchain.info after this?

Speaker??? Knockertz - January 1, 2015, 2:31 am

(Jan 1, 2015 03:28 AM)Autocorrect Wrote: [\[CITE\]](#) <https://lastpass.com/>

Makes long passwords a lot easier.

Encryption is mandatory if you're paranoid.

I saw your post in the graphics section where you roasted grievous. Shit was pretty alpha.

Autocorrect - January 1, 2015, 2:32 am

(Jan 1, 2015 03:31 AM)Childish Gambino™ Wrote: [\[CITE\]](#) I saw your post in the graphics section where you roasted grievous. Shit was pretty alpha.

Was that on the thread about the new business group? ?

420 Blaze It - January 1, 2015, 2:33 am

Thanks for the notice, I should act on this now.

Speaker??? Knockertz - January 1, 2015, 2:36 am

(Jan 1, 2015 03:32 AM)Autocorrect Wrote: [\[CITE\]](#) Was that on the thread about the new business group? ?

Yes. I laughed my ass off. Great job.

Regular Guy - January 1, 2015, 3:01 am

(Jan 1, 2015 03:30 AM)Moen Wrote: [\[CITE\]](#) I am sorry for your loss, Are you gonna limit your use of blockchain.info after this?nope... it wasn't my fault, i've taken proper precautions. I only lost around .4BTC, he lost majority of his BTC. It isn't my fault, I won't wear the blame. I'm just here to warn you

all.

Sure this fucking pissed me off as the only reason we joined wallets was because:

1. he wanted control (he didn't trust me)
2. wanted to monitor all activity
3. Thought it was safest with him
4. we were (and still are) running a project together

So, at least this goes to show you're better trusting your partner than an online wallet lol. Karma??

(Jan 1, 2015 03:27 AM)Childish Gambino™ Wrote: [\[CITE\]](#) My password is like somewhere around 40-45 characters lol it takes me a while to get in.

Good idea. also enable larger key stretching so it's impossible to get bruteforced, saw that in account settings today.

(Jan 1, 2015 03:25 AM)Autocorrect Wrote: [\[CITE\]](#) Why would you store so much BTC in a hot wallet?

For starters, it's not all my BTC. I still have digits stored in cold offline for 3~ years from now. Also as stated in OP for this exact reason I use many blockchain wallets. The only difference with this one was my partners was not as secure as I thought.

Shed - January 1, 2015, 1:19 pm

Damn..

And I just maked this

<https://hackforums.net/showthread.php?tid=4614299>

Will be downloading the offline wallet this night....

My Grandad Bombed Asia - January 1, 2015, 1:20 pm

I have SMS verification on my 2 factor, it's cool. I hope.

G^NNicus - January 1, 2015, 1:40 pm

I have to lost BTC on Blockchain...due to hackers.

I still use it, but nothing over 50\$.....

Deform - January 1, 2015, 4:19 pm

I'm gonna guess that blockchain is probably just taking peoples money now that people realize its not secure, take profits and leave.

~Jay~ - January 1, 2015, 4:29 pm

Yeah, Blockchain.info has been proven to have a lot of security issues. I'm sorry for your loss, but you really should have taken the massive amounts of money that were getting stolen as a warning sign.

Divined - January 2, 2015, 3:35 am

Uhm, I always thought that blockchain uses identifiers and such? Although I knew a guy that was able to hack blockchain wallets, I wonder how. I mean, bruteforcing sure, but how do you get past identifiers?