

https://www.reddit.com/r/Bitcoin/comments/t4mwqr/i_get_hacked_24_bitcoin_stolen_from

MAR

FEB

MAR

2022

2025

2026

06

06

06

Log in

Log in

Log in

3 captures

2 Mar 2022 - 6 Feb 2025

About this capture



r/Bitcoin • 3 yr. ago
red123qwer



I get hacked, 2.4 bitcoin stolen from coinomi wallet

hello,

On 28feb2022 I get hacked, 2.4bitcoin from [u/coinomi](#) android wallet got stolen.

It's an old Android 7, Samsung Galaxy s6edge (no root).

In 2017-2019 I use [u/Coinomi](#) wallet to store my bitcoin because was simple easy to use.

In summer 2019 I decide to use that phone only like a "cold storage" I have [u/coinomi](#) app, windscribe vpn and google apps. I choose that because was simple , once a month I power the phone do the update on [u/coinomi](#) and the other apps checking the wallet and shut it down.

The [u/Coinomi](#) wallet do not have the BIP39 passphrase implement ate at that time but I secure the wallet with a password , with a pin number in case somebody had the phone to be hard to unlock it.

At the end of February2022 I update the [u/coinomi](#) wallet to version 1.25.2 build 430 core 220 all work fine update done, I check the wallet the bitcoin was there (I also choose the feature " Mark do-not-spend " in case somebody open the wallet no amount was display) but today I check the address of my wallet (I have it saved in tor browser to be simple to check the utxo) and I see the coins were moved

<https://oxt.me/transaction/812f73d94bc1eb029e72930427ea27bee4e668accaad4d3fc167a24f1de364a5>

how can this happen ? since nobody have access to the phone.

The seed was stored on paper ,nobody see it ,plus I wrote the words in other order so only I can know the right order.

I'm sure something was wrong with the update since is not an open source wallet nobody knows what that wallet can send out butt I think the wallet send the seed out to somebody because passed 3 and half years and the seed was safe inside it only know happen..only after the update.

After 5 hops I saw the bitcoin Is sent to Binance exchange address

<https://oxt.me/transaction/2984598d66601f7cf922f819b32da464733ec00bd5e71ce76ca6627fdc97e38f>

do not have a binance account but I chat with them to the live chat:

Greetings from Binance security team! We are very sorry to hear about your situation. Upon checking we have found that the funds are in Fixed Float wallet.

The funds appear in the blockchain to have been sent to Binance because Fixed Float is a Binance Broker, this means it is another company that has a wallet with Binance for its liquidity and order book. This broker has many users, so we don't know the exact end user who received your stolen funds, we only know the funds were transfer to the Fixed Float hot wallet.

Skip to main content
3 captures
2 Mar 2022 - 6 Feb 2025

MAR 2022
FEB 06 2025
MAR 2026
Log in
About this capture

perfect and they are on the market since 2014 and nobody have issues, some years ago I remember a guy that also lose funds from coinomi desktop wallet was a big fuss then but nobody believe it neither I but now I think something is not ok.

My question is how can somebody take the seed from the wallet if that wallet was shut down 95% of the time since summer 2019 ?

I was careful with the coinomi app , always FORCE STOP and only open the app if the VPN was on.

For me is very strange that my bitcoin was stolen after the update.

That update had something that read the seed and sent it out, I can't see other explication.

I just wanna share my experience , I do blame the guys that work on Coinomi , they always say [i]the wallet is safe nobody lose funds it's impossible to be able to see your seed [/i]but the app is not open source so how can this be true ?

Via support ticket they wrote me this:

After looking through the details given we can confirm the transaction was sent from a device where Coinomi was installed. However, due to the nature of cryptocurrency transactions we cannot say 'whom' made this transaction since we are a non-custodial wallet software which means we do not track any sort of user data.

Coinomi is one of the most widely known multicoin wallets and also one of the easiest to use. This means it is more likely than you think for someone to select to restore any seed into Coinomi

Please could you tell me, do you access the app from the same IP all the time? Do you use a VPN?

FixedFloat reply via email:

We're sorry that you were subjected to theft of funds.

FixedFloat is an instant non-custodial exchanger. After the receipt of funds and the receipt of the required number of confirmations, the exchange takes place immediately.

We do not require any personal data for the exchange. We can only request a search of the server logs (IP, user-agent, language) from our technical specialists. But we need an official request from your regional police or other representative, from their official email address in order to issue confidential information.

After receiving an official request from law enforcement, we will be able to send server log data and order data.

Unfortunately, this is the maximum we can help in this situation.

I post this story on reddit they close the post, If i wrote on they telegram group they tell me to stop because the wallet is good.

I think was an inside job.. or can somebody tell me how the hacker get the seed from a wallet that is power off almost all the time?

One of the biggest loss of my life.

Here you can see how the hacker move the bitcoin

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06

Log in



2022

2025

2026

About this capture

<https://oxt.me/transaction/b266a2d1d586f0bcb3bd6c1003969b0930382531d0c166755fd1ed1a1aa5cbc0>

<https://oxt.me/transaction/67b8563a226c864c12fd059b5ca29f2c9ccb556958b08b2ada1a5de79c6aa677>

and then In [u/binance](#) [u/FixedFloat](#)

<https://oxt.me/transaction/2984598d66601f7cf922f819b32da464733ec00bd5e71ce76ca6627fdc97e38f>

TRANSACTION

812f73d94bc1eb029e72930427ea27bee4e668accaad4d3fc167a24f1de364a5

MONDAY, FEBRUARY 28, 2022 8:25 AM [BLOCK 725250]

SUMMARY

INPUTS & OUTPUTS

TECHNICAL

NOTES (0)

ANON-3954344504 [bc1qgeuq8...]

-0.98000000 B

ANON-3954344504 [3fYmUKpF...]

-0.10000000 B

ANON-3954344504 [bc1q3qvku...]

-0.10000000 B

ANON-3954344504 [bc1q4ysks...]

-0.24000000 B

ANON-3954344504 [bc1qkzrm...]

-0.98000000 B

ANON-3954344504 [bc1q2q4yn...]

-0.94000000 B

ANON-3954344504 [bc1qftlp3...]

-0.30000000 B

ANON-3954344504 [bc1q6mydd...]

-0.20000000 B

bc1qee3erwmsqf8zpew84mimym83w82ngxo0f9...

2.39991369 B

VOLUME OUT

2.39991369 B

FEES

0.00008631 B

TOTAL

2.40000000 B

TRANSACTION

59448820438e21501673e6c732419a3f1b9a04fcoe086ab3638c58238348b0b6

MONDAY, FEBRUARY 28, 2022 9:38 AM [BLOCK 725253]

SUMMARY

INPUTS & OUTPUTS

TECHNICAL

NOTES (0)

bc1qee3erwmsqf8zpew84mimym83w82ngxo0f9...

-0.00505847 B

bc1qee3erwmsqf8zpew84mimym83w82ngxo0f9...

-0.00595656 B

bc1qee3erwmsqf8zpew84mimym83w82ngxo0f9...

-0.01274646 B

bc1qee3erwmsqf8zpew84mimym83w82ngxo0f9...

-0.01380000 B

bc1qee3erwmsqf8zpew84mimym83w82ngxo0f9...

-2.39991369 B

ANON-3954902334 [bc1q297gx...]

1.20000000 B

bc1qddsqmvgkhqzw9dfe4pyssavq8kexj3an3...

1.23747846 B

VOLUME OUT

2.43747846 B

FEES

0.00001672 B

TOTAL

2.43749518 B

Skip to main content
3 captures
2 Mar 2022 - 6 Feb 2025

MAR 2022
FEB 06 2025
MAR 2026

Log in
About this capture

MONDAY, FEBRUARY 28, 2022 9:52 AM [BLOCK 725256]

SUMMARY INPUTS & OUTPUTS TECHNICAL NOTES (0)

< bc1qddagmvmghkqqr8dfe4pyssvqdxj3an3... -1.23747846 B

bc1qgqqrw9jw4jqp3amqc8753u74c7az4nej... 0.10000000 B >

bc1qctjyqjw3fjy3jth0uk39uk79ka27xdt9v0u... 1.13746978 B >

VOLUME OUT 1.23746978 B
FEES 0.00000876 B
TOTAL 1.23747846 B

TRANSACTION page 0

5bc73935ea9122efbf3c1bd9f5a7dffd5dcf57b5ad79b65430725d016a1d4b3

MONDAY, FEBRUARY 28, 2022 10:56 AM [BLOCK 725265]

SUMMARY INPUTS & OUTPUTS TECHNICAL NOTES (0)

< bc1qgqqrw9jw4jqp3amqc8753u74c7az4nej... -0.10000000 B

bc1qgqqrw9jw4jqp3amqc8753u74c7az4nej... 0.01471300 B

ANON 3954574234 [bc1qCq45...] 0.08528537 B >

VOLUME OUT 0.09999942 B
FEES 0.00000158 B
TOTAL 0.10000000 B

TRANSACTION page 0

5bc73935ea9122efbf3c1bd9f5a7dffd5dcf57b5ad79b65430725d016a1d4b3

MONDAY, FEBRUARY 28, 2022 10:56 AM [BLOCK 725265]

SUMMARY INPUTS & OUTPUTS TECHNICAL NOTES (0)

< bc1qgqqrw9jw4jqp3amqc8753u74c7az4nej... -0.10000000 B

bc1qgqqrw9jw4jqp3amqc8753u74c7az4nej... 0.01471300 B

ANON 3954574234 [bc1qCq45...] 0.08528537 B >

VOLUME OUT 0.09999942 B
FEES 0.00000158 B
TOTAL 0.10000000 B

I scan the phone with malwarebyte and is all fine

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR 2022

FEB 06 2025

MAR 2026

Log in

About this capture

Scanner

✓

No malware found!

382	3730	02:19
Apps scanned	Files scanned	Time

Previous scans

● On-demand scan

Mar 2, 2022

Scan completed in 02:19

Scanned: 3730 files 382 apps

● On-demand scan

Feb 23, 2022

Scan completed in 27:49

5/38

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

2022

FEB

06

2025

MAR

2026

Log in

About this capture

Kaspersky malwarebytes mcafee eset noothing

hey [u/coinomi](#) why the app connect to this stranges ips 188.144.96.7
<https://whatismyipaddress.com/ip/188.144.96.7>

Decimal: 3163578375

Hostname: 188.144.96.7

ISP:

Organization:

Services: None detected

Assignment: [Likely Static IP](#)

Continent: Europe

Country: Germany

[151.101.1.195](#)

Decimal: 2539979203

Hostname: 151.101.1.195

ASN: 54113

ISP: Fastly

Organization: Fastly

Services: None detected

Type: [Corporate](#)

Assignment: [Likely Static IP](#)

Continent: North America

Country: United States

State/Region: New York

City: Brooklyn

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR

06

Log in

2022

2025

2026

About this capture

↑ 105 ↓

🗨 211



Share

Sort by: Best ▾

🔍 Search Comments



satoshisfeverdream • 3y ago

A cold wallet that you put online once a month to update apps? Not sure that's how cold wallets are supposed to work.

Not trying to kick you when you're down but if you have \$100k+ maybe spend \$50-100 on a dedicated hardware wallet to store it.



↑ 87 ↓



ncsakira • 3y ago

most likely one of the apps had malware? maybe even the AV scanner, or the some phone bloatware!

op should post phone brand and model as well as a full dump of all the apps installed.

↑ 10 ↓



red123qwer OP • 3y ago

I know what you say.. was my mistake that I didn't do it..UI trust the wallet that all will be fine.for 3 years nothing bad happen only now.

in 2017-2019 those bitcoin don't have a bigger value ..I just left it there because...well I'm stupid (I agree with this)

I was sure all my methods work, using a vpn, keeping the wallet with just minimum apps, not internet traffic ,no chat apps, phone was shutdown 99% of the time in last 3years

If somebody had the seed before when bitcoin was 65k why they don't do it?

they do it now because now they got the seed , they have it after the last update of the wallet.



↑ 9 ↓



Blade2075 • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

ever accessed wallet on public wifi you also could have got hacked that way.

You made a mistake in having that phone accessible to the Internet. Cold wallet means 0 Internet connection.

Sorry man 2.4 BTC is big loss and chances of recovering it are close to 0%. The faster you can learn and accept it the better. And BTC has many room to grow. If you keep investing you will recover losses and be in the green again.

19



red123qwer OP • 3y ago

Was that good bitcoin that I DCA when was under 10k ..that will never happen again. I feel like my time was stolen..time that i work to get money and put it all in bitcoin.

thank you for you mesage

15



TakeMyBoomerMoney • 3y ago

Your time was not stolen if you've learned a lesson. In your case, a valuable lesson, but not THAT valuable.

There are far more important things than money.

I hope you manage to continue with your life, learn the lessons and put the past behind you. look to the future.

What comes around goes around. Don't worry, what you lose, you gain in some other way.

good luck!

8



[deleted] • 3y ago

VPN won't stop a key logger on your phone. Antivirus won't work if you have a virus that is smarter than it. Older phones have more vulnerabilities then newer phones.

An exchange with 2/3FA would have been safer then this.

5



lacksfish • 3y ago

Did somebody have access to the phone? Maybe you threw a party and it was in the drawer? Maybe a friend of a friend of someone you know visited you and had a chance to to start the phone and export the backup phrase?

2



red123qwer OP • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

The only people that knew that I use coinomi wallet and I have bitcoin there is the coinomi team that create the app.

4



lacksfish • 3y ago

Did you write down your secret backup word phrase? If so, where did you store it? Could anyone have had access to that?

4

8 more replies



u/sloaleks • 3y ago

I have bitcoin there is the coinomi team that create the app.

Actually, they don't. It's called a non custodial wallet for a reason. Only you know.

3



reddito321 • 3y ago

Sorry for your loss. I myself can't imagine having 2.4 BTC and not putting it in a proper hardware wallet.

152



eld101 • 3y ago

This sums it up.

53



red123qwer OP • 3y ago

I know but was there since 2019 easy to access ..2.45bitcoin was not that much at that point.

I know is also my fault but is also strange that the hack was done after tthe last update of the wallet.

If soomebody had the seed before he will not wait till now to do it

13



dlq84 • 3y ago

You had a \$200k on your phone, even in 2019 it would have been worth paying \$150 to properly protect it.

40



chillinewman • 3y ago • Edited 3y ago

Hardware wallet not a phone, is very possible is the coinomi update, do you have the IP of where the update came?. Some malware won't show in scanners without root access.

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

update come from google play store.

2



chillinewman • 3y ago

Did the IP belong to Google? Hackers can fake updates. Also it could be coinomi itself

2

3 more replies



chillinewman • 3y ago

See an example of a fake update: wallet stealing app.

<https://arstechnica.com/information-technology/2022/03/google-play-app-drops-data-stealing-teabot-rat-on-10000-android-phones/>

1

2 more replies



CombJelliesAreCool • 3y ago

Yeah it was easy to access, thats for sure :/

That sucks bro, sorry for your loss. I hope this doesnt deter you from moving forward and stacking. You receiving two \$13000 transfers in one year makes me think youve got some money coming in so I wouldn't think so but you never know.

7



Entebe • 3y ago

July 24, 2019 the price was around 10k USD. Those 0.3 BTC are worth 13k now.

4



nullama • 3y ago

In summer 2019 I decide to use that phone only like a "cold storage"

Any device that is connected to the internet is not cold storage.

There are a multitude of ways in which a hacker can steal your funds if your device is connected to the internet.

Cold storage means no connection to the internet, and it's the safest way to keep your bitcoin.

You can setup a watch-only wallet in an internet connected device to interact with your cold wallet easily.

37



saltyblueberry25 • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

5



CoolioMcCool • 3y ago

It's not hard. Ledger and Trezor are both really easy to use.

6



nullama • 3y ago

Electrum can do both. [You can even use a raspberry pi zero as the hardware wallet](#)



8



hemzer • 3y ago

Why pi, Can you not just use a USB with TAILS OS offline PC boot with USB and follow <https://electrum.readthedocs.io/en/latest/coldstorage.html>

1



nullama • 3y ago

Of course you can.

I prefer the Pi Zero because it's a fully working computer itself(with the USB you need a separate computer), and it doesn't have networking hardware (no wifi, no bluetooth).

1



Taz7877 • 3y ago

Try mycelium very good watch only wallet

1



[deleted] • 3y ago

Electrum, very easy to do and put in cold storage. Just need an offline computer that never goes on the internet

1



coinomi_brenny • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

would be thousands more reports of such from the latest application update and there are still many more people holding more than 2.4btc in the Coinomi app (We get many users daily in our support channels holding much more) so would they not have been prime targets?

Whilst it is always a sad thing to hear when a user loses funds. The evidence provided points towards either;
A) an infected/breached user device. Activity sniffer/loggers which have taken passwords from the user device or have used another "0 day exploit" to remotely control the device. or
B) a compromised recovery phrase backup which this user claims was written on paper.

18



cjeans23 • 3y ago

I can only imagine how bad it will get when technologies and computers advance. This is one of the issues QAN is tackling through their blockchain.

So sad for OP losing that huge amount of money.

3



DankShibe • 3y ago

Open source your app please. There are multiple other ways to combat malicious app reproductions .

1



[deleted] • 3y ago

It was an inside job, this has happened before. I would suggest OP to file a digital crime claim with their local police, this is a very serious case.

<https://www.avoid-coinomi.com/>

1



coinomi_brenny • 3y ago

It is not an inside job. The link you provided links to an old story where a user tried to blackmail and extort our company. We already told the OP to report this activity to his local police so they can begin contacting exchanges and centralised services to have the funds blocked there.

2



SenatorAstronomer • 3y ago

I'm sorry for you loss, truly am. But anyone else out there keeping your coins in a hot wallet, just spend the money and get a hardware wallet. .0032 can get you a decent cold storage wallet! Just do it!

16



u/Inevitable-0246 • 3y ago • Edited 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR

06

06

06

Log in

2022

2025

2026

About this capture

- cold storage - substantial BTC holdings are better held via a mechanism that is truly cold and has no access to interact to/from the internet. Only have watch-only wallets on connected devices.
- seed phrase - take the security of seed phrase seriously, exposure of your seed phrase (with passphrase if there is one) means your holdings is accessible by others!
- open source - whilst it does not guarantee security, at least there is some better transparency on what's actually in each software release and not solely relying on the words of the software developer.
- avoid mixing BTC with alts - more for those who have substantial BTC holdings yet also have some alts - beware of compromising on what you could do to securely hold your BTC for the convenience of having a single software / device for BTC + alts. Consider is the convenience really worth exposing your substantial BTC to the added complexities / risks of multi-blockchain mixed code base behind the software / firmware?

8



red123qwer OP • 3y ago

Agree with all your points

I know [u/coinomi](#) is a app for alts but I use it for bitcoin because design is easy but is not open source and this is the big problem.

3



Inevitable-0246 • 3y ago

Personally I have more BTC and only limited alts. BTC mostly held via Coldcard never connected, with watch-only on BlueWallet plus a small stack held via BlueWallet for easy outbound transfers.

I don't have self-custody for alts yet and still figuring out if I could implement a similar pattern, an air-gapped hardware wallet supplemented by a software wallet that can also do watch-only. But I would shy away from using the same solution for BTC vs alts....

Thanks for sharing re Coinomi, it's on my list to investigate but if not open source, off the list it goes.

2



Mordan • 3y ago

but is not open source and this is the big problem.

complete failure of judgement sorry for your loss.

I write software and its easy easy to steal with updates.. I REQUIRE THAT PEOPLE DOWNLOAD SOURCE CODE AND COMPILE for anything Bitcoin related.

2

[deleted] • 3y ago



Romando1 • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture



Mordan • 3y ago

NEVER UPDATE APPS.

DO NOT TRUST> VERIFY.

Take extensive measures to check updates.. Weeks if not months.

Every update is potentially a virus or a trojan.



2



BlueberryDefender • 3y ago

Is it possible for trezor firmware updates to be a Trojan? There seems to be frequent updates through trezor suite



3



Mordan • 3y ago

Is it possible for trezor firmware updates to be a Trojan? There seems to be frequent updates through trezor suite

ouch.. Yes updates can be malicious. Its an easy attack vector.

CIA storms the building. Points a gun to your head. Tells you to apply this nice little update provided by said CIA. Bam. You are fucked.



1



red123qwer OP • 3y ago

do it.don't wait and trust a mobile wallet



1



SuperSan93 • 3y ago

Scammers and hackers for profit are truly some of the worst people to exist. I'm sorry to hear about this.



13



red123qwer OP • 3y ago

thank you

I'm curios how they do it



2



[deleted] • 3y ago

Isn't it clear? You used an old, outdated android phone as a hot wallet.

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

but how exactly they do it ?

1



[deleted] • 3y ago

How would we know? We don't have your phone and can't inspect it.

1



Mallardshead • 3y ago

One thing I never trust are "multichain wallets" like Coinomi. Those things have endless attack vectors. Next time use a bitcoin only wallet. That goes for hard wallets as well. As well, don't ever store large amounts of bitcoin on anything connected to the internet, like a phone or paper wallet.

It was definitely the update.

13



coinomi_brenny • 3y ago

Hi there, Coinomi is non-custodial and never has access to user funds. The recovery phrase/keys never leave the user device. We are speaking with this user to try and help them figure out how it may have happened. Thanks

8



ethereumfail • 3y ago

how would anyone know that if your app is closed source lmao

thank you guy in charge of bank of coinomi that adds fake projects like premixed eth, go scam yourself

3



2Panik • 3y ago

These VPN's are another way to monitor an log what you do. Don't exclude that possibility.

9



u/r red123qwer OP • 3y ago

I know that but how can the VPN go inside the wallet and take the see? seed is [aes256 encrypted as cooinomi dev say](#)

2



Kezuma • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

I don't know what happened, but connecting to a VPN for stuff like this is a huge security hole, especially if the android version you used has a known vulnerability.

VPNs are for accessing specific networks that you cannot access otherwise. They do not improve your security or provide you with any privacy. They do the opposite.

Also, cold storage should not touch any network, get an actual hardware wallet!

↑ 3 ↓ ...



Pacman_Frog • 3y ago

Depends. If you use a VPN you see advertised on TV you have no security.

↑ 1 ↓ ...



ethereumfail • 3y ago

they can say anything, it's still closed source and no way to check where else the key might be

↑ 1 ↓ ...



akaryuDeb • 3y ago

I see big security flaws here. I am really not an expert on cyber security, but those are kinda the basics.

1. Do not connect your cold wallet device to the internet. You lost the BTC in you HOT wallet, which is still a bummer but it isnt something impossible to happen.
2. Never use a VPN*, you are just handing over your data to their server. Nice service to have if you want to be anon, but you are basically trusting the people who own the server not to sniff your data. There is no need in using a VPN unless you arent able to access internet without it. And if you need to use it, pay for it and use the most reputable service.
3. Never use an old phone as hot wallet. The problem is in the software, Android 7 is pretty old and probably full of 0 days exploits (aka they can hack your phone and access it without you even touching anything). Since security patches are not delivered on older androids, it is easier as the time passes to find one cheaply.

What could have happened: Step 1: You use said vpn to access the internet and by doing so you provide the information about your btc holdings and your device. I think the update has nothing to do with it, every time you connected through the vpn you risked someone else sniffing your traffic. Step 2: then the used a 0 days attack and gained access to your device.

Maybe the hacker did step 1 way back and just waited you to connect again in order to proceed with step 2. Sure there are many other ways, this is just one i thought of being possible.

⊖ ↑ 4 ↓ ...



red123qwer OP • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

Simply by passing all the PIN/password I have on wallet

This is the only solution I have in mind now.



akaryuDeb • 3y ago

You don't understand how things work. Being not open source doesnt mean in any way that they can read the wallet seed or that they can send it away. It is actually impossible for them*. Closed source means that they own the code and it is not public, *sure they can add a hidden feature to steal your assets but then you would not be the only one victim and people will realize the scam.

I literally told you how the hacker could have gotten away with your btc. Search "0 days exploit" on Google. Basically they can enter your phone without the need of you downloading a virus or opening a link. The hacker after getting in you phone just needs you to type your wallet psw using a keylogger (or just bruteforce it) and there you go they have your seed.



ethereumfail • 3y ago

there's still no source to check and if you did have a way to see your users private keys in your closed source app they could just take advantage of taking coins from very few users at a time. Note that it wasn't few 100 bucks they stole, but over 100K worth.

if you are going to trust closed source wallet, might as well trust a bank



akaryuDeb • 3y ago

Lets start by saying that i only use open source wallets if i can choose. And i never told that you should use it.

The fun part is that MOST of people like you saying that "closed source wallet are stealing your money" are not able and wont ever check the code of their open source wallet to see if everything is all right. You cannot prove whose fault it is, there is no point in accusing anyone unless you find evidence.



+ 2 more replies



DankShibe • 3y ago

S6 is 7 years old. Haven't get a single update from Samsung in the last 4 years. If such an outdated device connects to the internet it once, consider it compromised.



red123qwer OP • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

My conclusion is that after the last coinomi update they do something and send the seed out

1



DankShibe • 3y ago • Edited 3y ago

There is another set of keys that are beeing used to decrypt and encrypt your AES256 seed phrase. This is what allows you to facilitate transactions. They are called encryption keys.

Point is , that even if coinomi wanted to steal from you , if you had a galaxy S21- s22 and enabled biometrics , they would not be able to, because the phone itself would securely store the keys to decrypt your seed phrase from the 256AES encryption and coinomi or any wallet that has that feature , would not be able to.

Also your phone might be infected somehow and hackers were able to take your seed phrase or control the coinomi app remotely. Google play store itself has security updates as well. You might even have downloaded a hacked coinomi because your play store itself was out of date.

Since it is very old, it doesn't protect from newer attacks. There was also the specter and meltdown hardware issue.

<https://oneandroid.net/how-to-know-if-your-android-will-receive-the-patch-for-meltdown-and-specter/>

Phones are much harder to hack than PCs in general. And I have heard people storing 100k+ USD in their PC using a software wallet without issue. 😊(It is wrong to do that , but just saying)

1

2 more replies



iammassvidal • 3y ago

You can connect cold storage device while computer is connected to internet that's the whole point of a ledger trezor or HW. That's the point of the device it protects the seed.

2



akaryuDeb • 3y ago

And? What are you trying to say?

2



MiserableEgg0 • 3y ago

please DO NOT reply to any dm offering help to recover your funds!

So sorry to hear about your loss, your funds are most likely gone I wouldn't imagine if myself had 2.4BTC And stored them in a hot wallet

7



red123qwer OP • 3y ago • Edited 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

ps: I already get a DM

↑ 12 ↓ ...



dextersh • 3y ago

You have 383 android apps on that phone!? Bruh...

⊖ ↑ 7 ↓ ...



red123qwer OP • 3y ago

that's the total amouth oof apps that android have. it count every single app.

You realize that is impossible to install 383 apps? there is no space for that many apps

⊖ ↑ 2 ↓ ...



dextersh • 3y ago

Ah OK I see. My phone seems to have a similar amount actually now that I scanned it.

↑ 3 ↓ ...



Stocksugardaddy • 3y ago

Sorry to hear about your loss. If the hackers found an exploit in that wallet a lot of people are going to be out BTC by this time tomorrow.

↑ 3 ↓ ...



symmiR • 3y ago

This is so sad :(

↑ 3 ↓ ...



InvestWise89 • 3y ago

I don't use this app, but to get it right: You did put your seed in there (at least one time) to see your funds? Or did you only put your public address in there, like when you check it in your browser?

Many say "buy a cold wallet device" like a trezor, but i would prefer to use paper wallet and an offline notebook for any transaction. You have to learn, how this works and it will take a little bit of comfort away. But this method is 100% save.

If you know how (there are many tutorial out there), your seed will never be used on a device with internet connection. This made it 100% secure.

↑ 3 ↓ ...

The_Zorbi • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

5



Mordan • 3y ago

Any of those apps (via malicious update)

Pro Tip: NEVER UPDATE ANYTHING IF YOU HAVE CRYPTO ON THE DEVICE.

Updates are potential trojans.. rug pulls or hacks.

-4



joecool42069 • 3y ago

Horrible advice.

Just don't store your coin in hot wallets. Your phone is literally a computer on the internet.

10



Mallardshead • 3y ago

Your seed was written down. Where did you keep it exactly?

And the update, were you prompted to do the update by the app?

2



red123qwer OP • 3y ago

The seed was in a secure place, even if you had the seed was hard to guess because I change the words order and only I know the exact order.

Ironic.. I update the app to be secure *up to date and safe*

1



Mallardshead • 3y ago

Ok, so it was the update then not the seed. Where did you find the update? Can you go back into your phone and find the update?

4



[deleted] • 3y ago

I don't know how it could have leaked you seed. It most likely was a malicious update to the app. Once the app is compromised it can send data directly to their servers somewhere and your funds are gone.

I would highly recommended a coldcard or another specifically designed cold storage device that is never connected to the internet. At least for the bulk of your funds. You can use a phone app for day to day amounts but the majority remains in cold storage.

2

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

this.

NEVER UPDATE. DO NOT TRUST! VERIFY!

I bought a new nano ledger because I didn't want to update. I don't trust the process.

2



BlueberryDefender • 3y ago

You mean you didn't want to update the nano ledger firmware? So you're planning on buying a new nano ledger (loaded with newest firmware) whenever there is a firmware update? Genuine question.

1



Mordan • 3y ago

So you're planning on buying a new nano ledger (loaded with newest firmware) whenever there is a firmware update? Genuine question.

yes. that's my current strategy. considering the value on it. I don't take any stupid risks and updates are IMO one of the biggest risks ever.

But I won't use ledger anymore. They are like a bank now.. You have to connect to their centralized online service to even look at your coins.. They know everything about your wallets. Ledger Live is convenient// But its like a bank down the road.

2



BlueberryDefender • 3y ago

Which hardware wallet will you be using in the future then? And how are trezors?

1

1 more reply



Mrs-Lemon • 3y ago

I bought a new nano ledger because I didn't want to update. I don't trust the process.

This is totally crazy, unnecessary, and actually a huge security flaw.

One of the least secure actions is actually entering a recovery seed. This is how people lose their coin 99.9% of the time.

If you don't trust Ledger, then use a different cold wallet.

1



Mordan • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR

06

2022

2025

2026

Log in



About this capture

you lost me there buddy.

First of all, there is no "recovery" seed. There is a seed that generates wallet addresses. So that security risk of managing your seed is irrelevant to the ledger. That seed can be used in any compatible software like Bitcoin Full Node.

I trust ledger to not leak the seed on brand new packaged products. But I don't trust the updates.. That's a whole different thing. Its philosophical. Updates are big attack vectors.

Updates bricks Bluetooth devices on purpose for example.. Updates make computer slower on purpose etc etc.

0



Mrs-Lemon • 3y ago

If this loses you then I suggest you do more research. Most people lose their funds by typing out their recovery seed in what they think is a ledger/trezor interface but actually it's not.

If you don't know this than you haven't researched how people lose their funds on these devices well enough.

Either way, handling and entering your recovery seed is the most risky thing you do in under normal operation.

Call it a seed or recovery seed. I don't care. Risk is the same.

What you are doing is extremely risky.

1



2 more replies



red123qwer OP • 3y ago

That's what I'm saying the update leak the seed.. why just now and not before ?Tthis happend after the update..the update I make it from google play store

1



[deleted] • 3y ago



WaYYne169 • 3y ago

I'm sorry for your loss.

2



FiveYearCryptoPlan • 3y ago

Blag update, I had an #update from supposed Binance, clicked it, crippled my phone

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR

Log in

?

X

06

Log in

f

t

2022

2025

2026

About this capture

 b0ddenb00s • 3y ago

You probably know the saying "don't trust, verify" that implies don't trust anything you can't verify. Therefore don't trust anything that isn't open source

↑ 2 ↓ ...

 metulburr • 3y ago

You said you used your phone like cold storage. Except your cold storage wasn't really cold storage. It's a hot wallet because it can leak your seed to the internet. Thr loss was unfortunately due to negligence. Next time use real cold storage and buy a Ledger or Trezor

⊖ ↑ 2 ↓ ...

 u/red123qwer OP • 3y ago

that's the word **negligence** and I assume this mistake, like what else I can do? just share my story so others don't trust blindly a close source wallet app

⊖ ↑ 2 ↓ ...

 metulburr • 3y ago • Edited 3y ago

And I am sharing the method of how to not lose crypto. So when readers read this they know there is a safe way to hold bitcoin. And it's not any hot wallet period. If you can connect it to the internet it is at risk. Which is every and any type of hot wallet. Cold storage would protect the seed.

This is the golden rule of crypto... "If you can connect it to the internet it is at risk." That is any phone, tablet, computer, etc. Any hot wallet is subject to leak it's seed by either the user or the company that made the wallet. The only safe way to hold crypro is to use cold storage such as ledger or trezor in which they protect the seed from the internet. Hot wallets do not do this. You don't need your phone on for someone to gain access to your seed and take your crypto from a hot wallet.

↑ 2 ↓ ...

 gbhaddie • 3y ago

Tangem for cold storage is what I like.

↑ 2 ↓ ...

 carboonpn • 3y ago • Edited 3y ago

Dude I have much much less than you and I bought 3 ledger nano's and using multisig. Sorry for your loss but you're phone is comprised.

↑ 2 ↓ ...

 Coolster-crypto • 3y ago

Sorry to hear this. I got hacked on my coinbase cold wallet. Could never figure out how this happened.

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

AlexH1337 • 3y ago

Galaxy S6 Edge, unsupported for god knows how long, running Android 7, and completely missing years of **critical** security patches.

That's the kind of thing where you'd have out in the wild RCE / root exploits that require zero interaction. A passively compromised device like that (and no, "AV" apps won't help) leaks any app data, any data loaded in memory (that includes your seed phrase / private key the moment the app is unlocked).

Massive F. Sorry for your loss. I hope anyone reading this doesn't make the same mistakes. **If you insist (don't) on using a device like this, keep it OFFLINE.**

2 ...

u/r red123qwer OP • 3y ago

was offline all the time.just power on for max 5-10min do the damn coinomi app update.

Why this happen only after I update the coinomi app , I'm sure they stole it other option don't exist. If somebody find the seed then it should have the seed from other wallets I had but those wallets are untouched.

1 ...

AlexH1337 • 3y ago

Look, we can argue all day long. Exposing a device that is that vulnerable to the internet for any amount of time is pure russian roulette.

You won't be able to prove that coinomi stole your bitcoin given the glaring issue above, I won't be able to help you do that, and no one else can. That's the unfortunate reality.

1 ...

u/r Nada_Lives • 3y ago

With open source software, there are generally more eyes watching for exploits and backdoors.

Sorry to hear!

3 ...

coinomi_brenny • 3y ago • Edited 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

Unauthorized transactions can only be made by a) **someone who has access to your seed phrase**, or b) **someone with access to your device and knows your password**. There is no other way. We occasionally receive news of users having their email accounts hacked, giving attackers access to their seed backup files kept on their email or other cloud service. Please review your seed backup security, try to remember if you ever entered your seed on any other wallet, website, form, notes tool, etc; or check if anyone could have accessed the app on your device and knows your password.

One thing which concerns us the most is the use of the VPN on a device you claim is **"connected to the network once a month to update"** and is only used for coinomi. This does not ring true with the evidence you posted here, it shows **you have 300+ applications on your device** which would suggest some daily use on this device with this many apps it is becoming increasingly likely that one or more of **those apps are possibly stealing data from your device or logging some of your activity**. This coupled with the age of your device OS is a huge cause for concern.

We highly recommend you file a report with your local police/cyber crime unit so they can begin the task of reaching out to exchanges and centralised services in the hopes of blacklisting the funds for you whilst investigation takes place.

Kind regards.



[u/rred123qwer](#) OP • 3y ago

I already wrote all about the seed where I store it, nobody had access to the phone and I don't use that phone for daily use since 2019 when I get a new phone.

There are 382apps in total that's how android samsung come with many small apps..Malware bytes scan all of those

You cannot have 382 apps installed think logic. how can you use 382 apps?

Even if I had a keylogger app I don't unlock the seed that some app had the possibility to take a screenshot Malwarebytes

People should not trust [u/coinomi](#) because is close source app. and I'm sure the hack was done from last update..

You don't call me a layer and blame on me...yeah the blame is that I trust coinomi but you can't say that that phone was use for daily activities because was not.. is an old phone..not that fast with a small screen and bad camera that's why I stop use it like a normal phone since 2019.



[coinomi_brenny](#) • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

1. You may have stopped using the device as a daily driver in 2019 but you had already used the device online and it is possible one of the apps could have exploited you.
2. If someone uses a keylogger to save your spending password. They do not need to see the phrase once they have remote access to your device they can control and send as if they were you.



u/r red123qwer OP • 3y ago

the phone was shutdown when the transfer was made..the seed was send out from wallet.

there is not virus.keylogger in my phone. I scan it with antivirus

I never install apps outside google play

once again: if malwarebytes scan over 300 apps that's not mean I install 300 apps , that's something kinda fucked up to install 300 apps from google play, those apps are all from android system.

The seed was send it out from the coinomi wallet after the last updatte.

even if i my phone was compromise with a virus ,I didn't type that password since 2018 because I do not send bitcoin only receive

Wallet have a PIN, wallet have a password before sending.



u/r red123qwer OP • 3y ago

scan with Malwarebytes your android phone you should see over 300 apps scanned
Don't blame the number of apps from the phone. because the issue is not there.



u/r red123qwer OP • 3y ago

u/coinomi_brenny

Decimal: 3163578375

Hostname: [188.144.96.71](#)

SP:Organization:Services: None detected

Assignment: Likely Static IP

Continent: Europe

Country: Germany

why u/coinomi app connect to this static ip ?

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

Hi, if you would kindly edit your posts to remove/redact the IP details that would be appreciated. Respond on your support ticket for further discussion on every question you have so we can keep it all organised/documentated and to ensure we do not miss one of your many questions.

Your case is important to us and we will answer your questions in a correct manner. But please try to minimise comments such as "coinomi took my funds" or "it was an inside job" because this is unnecessary FUD.

Regards.



u/r red123qwer OP • 3y ago

is not a fud is a fact
the ip is public what do you want me to edit?

everybody can see that ip if they install coinomi wallet... and you still don't answer my question about that ip.



coinomi_brenny • 3y ago • Edited 3y ago

My concern about the information you are posting is simple. You do not know if any of this information could be relating to some bug or unknown vulnerability. Posting freely all of this without taking the correct approach of redacting things and responding to us in our private stream (ticket) you could be putting others at risk. If you did find a bug or vulnerability there is a procedure to follow to ensure responsible disclosure: <https://www.coinomi.com/en/responsible-disclosure/>

That being said, these are connections to our backend microservices which update balances and transactions, so nothing to worry about. These route through cloudflare for obvious reasons. The 151 IP is our connection to receive remote updates of the left side bar and OTA banners in the app.

Again, responding to your ticket with questions you have is the correct and best way to get faster replies and to ensure we do not miss your questions.



bnova21 • 3y ago • Edited 3y ago

Maybe someone did a SIM swap attack on your phone. . . That would give the hacker access to your phone number on a phone they control. From there they can reset passwords and gain access to your accounts.

<https://www.gemini.com/cryptopedia/sim-swap-attack-preventing-crypto-fraud>



u/r red123qwer OP • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

I'm not living in USA, I'm from east europe here we have not PC prepay sim cards.

I do not have a phone subscription.

0



dogstar_lordfly • 3y ago

At which point does it make sense to move to a cold storage?

1



Chipjack • 3y ago

Are you selling it this month? If not, put it in cold storage if it's currently worth more than you'd like to lose.

2



Mrs-Lemon • 3y ago

When you have a few thousand USD worth.

If you don't have cold storage now, then at least hold it on a top level exchange and disable withdrawals, only allow whitelisted addresses, authenticator apps, etc.

And if you do get cold storage, you need to understand that protecting your recovery seed is the most important thing. Never type it out. Ever.

If your cold storage device is asking you to type it out because of an update or connection problem, don't do it.

2



dogstar_lordfly • 3y ago

Thanks for the advice, I appreciate!

1



dlq84 • 3y ago

When you have more than 0

1



BlankEris • 3y ago

cold storage should be primary storage. only put in hot wallets what you intend to spend soon.

1



orbofdeception • 3y ago

problem is ur using coinomi

1

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

If you're using a phone that is no longer receiving updates, then you should have 0 expectation of security (and hence privacy), because it becomes trivial for any script-kiddy to exploit such devices using known, years-old (in the case of Android 7), unpatched vulnerabilities on your device.

You should have invested in a hardware wallet, or failing that, a secure phone like Google Pixels or iPhones (they're not perfect, but better than Samsungs, or other brands, which basically lag behind Google Pixels when it comes to updates; iPhones have stricter rules for apps, e.g. no IPC, unlike Android).

0



DankShibe • 3y ago

Newer samsung phones are on par , or even beat the pixels.Trading blows with Apple as well.

<https://www.publish0x.com/my-articles/samsung-s22-goes-all-in-crypto-with-brand-new-hardware-wallet-xppgrrp>

1



cryptobowzer • 3y ago

I feel sorry for your loss, but find it really hard to understand why you did not use a proper hardware wallet... Really confused that you allowed this to happen to yourself. Rule number 1 is not your keys not your coins

0



saltyload • 3y ago

Ha ha!

0



[deleted] • 3y ago



The_Zorbi • 3y ago

This is just speculation but based on what you wrote, I'd assume it's either the VPN provider (Windscribe, never heard of it) or someone close to you that knows about your funds. The most simple explanation would be that someone accessed your seed phrase that you wrote on paper (cleaner, friend, family member, etc.)

1



red123qwer OP • 3y ago

I don't know how the VPN can enter in my wallet and accesse the seed since the seed is encrypted. Nobody knew how many bitcoin I had and where I stored it..the only people that know is those from coinomi since they create the app if somebody have access thee seed they will use it long time ago not just now. I change the order of the words in seed so only I can know how tto read it

2

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture



red123qwer OP • 3y ago

I have Malwarebytes installed on phone, I scan it no issue found

Also with play protect say "no harmful apps found"



2



The_Zorbi • 3y ago

This study from 2019 lists Windscribe having 2 suspicious permissions on Android

<https://thebestvpn.com/android-vpn-permissions/>

Again, this is just speculation but I cannot think any other explanation for what happened. Like you said, if Coinomi had your seed, why would they empty it now?



1



Mrs-Lemon • 3y ago

I don't know how the VPN can enter in my wallet and accesse the seed since the seed is encrypted.

You enter your password to get into the app.

Anyone who has control of your phone and can key log it can access your coins.

Your seed being encrypted has literally nothing to do with it.



1



red123qwer OP • 3y ago

the phone was power off , when the transfer was made the phone was turn off

the phone was never let turn on without me touching the screen

Start the phone... update if was the case..doing a malwarebytes scan .>>>enter the wallet checking the bitcoin..force close the app..shut down the phone.

no virus no malware was find on the phone after i scanning



1



[deleted] • 3y ago

Sorry for your loss man.. it must be depressing. I'm not sure if a lawsuit can be filed towards an app developer against crypto hacks.

I want to appreciate you all sharing your experience and help us learn what to do/not do.

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR

06

Log in

?

x

f

t

2022

2025

2026

About this capture

I don't intend to open a law suite.... is my fault I trust a close source project

↑ 1 ↓ ...



dextersh • 3y ago

Sorry to hear that. Many google store apps are full of viruses by the way. Also I am pretty sure that a VPN can see everything you do, cannot be trusted. Also with so much BTC it would be good to spread it around like 5 different wallets on different devices just in case.

↑ 1 ↓ ...



Bitcoin__Hodler • 3y ago

never keep large sum of money ON YOUR MOBILE PHONE.

buy a hardware wallet.



↑ 1 ↓ ...



red123qwer OP • 3y ago

I don't have what to put in there anymore

↑ 1 ↓ ...



teamweeeman • 3y ago

The only phone storage I would trust is samsung. I wouldn't trust apps you can get from the play store. Those are hot wallets and vulnerable to attacks all the time. Samsung, while not a cold wallet, is not a hot wallet either. They have their own wallet built into the phone, secured and separated on the chip from the rest of the OS. I watched alot of videos and read up on samsungs wallet in their new phones, its pretty interesting stuff. If I was you I'd get a cold wallet.

↑ 1 ↓ ...



imagenxdude • 3y ago

Sorry to hear about your loss. I had coin stolen from a software wallet while trying my transition from an exchange to self custody. The wallet maker could not have cared less.

I am in the process of moving off Coinbase to use a BitBox hardware wallet. I've moved a small amount as a test and BitBox seems to work great. Before moving the remainder, I'm waiting on another device and a safe deposit box.

I want to ask what may be a dumb question. Is it possible to hack a hardware wallet app with a wallet app upgrade? Reading this thread made me wonder since I have to connect my hardware wallet to an app in order to use it. Any thoughts or suggestions about security would be appreciated.



↑ 1 ↓ ...

DankShibe • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

[deleted] • 3y ago



kwaker88 • 3y ago • Edited 3y ago

Sorry for your loss.

Edited: some info that I didn't do much background check, did not want to accuse anyone.

1



coinomi_brenny • 3y ago

Hi there, the posts you linked are irrelevant to this case. If you search for any other wallet you will also see reports of stolen or lost funds because, as we see day in and day out, people who are bad with their opsec need someone to blame instead of their own mistakes. Please stop trying to create FUD against Coinomi by linking old/irrelevant posts.

1



kwaker88 • 3y ago

Sure. I can delete my post. I apologize. I just wanted to give the op some closure.

2



thatmanontheright • 3y ago • Edited 3y ago

Timelines could match this story. <https://www.zdnet.com/article/cryptocurrency-wallet-caught-sending-user-passwords-to-googles-spellchecker/>

Somebody at Google resigned and took your money?

Edit - seems irrelevant since coinomi says it only applied to their desktop wallet..

1



red123qwer OP • 3y ago

I know the story at that time and I don't believe it but now.... things looks different.

1



coinomi_brenny • 3y ago

Hi, this post is irrelevant since it only affected the beta desktop release and forensic reports concluded this was not the cause of the user lost funds.

1



DisastrousFly1339 • 3y ago

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

↑ 1 ↓ ...



mike4score • 3y ago

Nobody took your seed, there was a virus from one of your 383 apps... virus used keylogger to get your coinomi password, then hacker just logged in and sent your funds away

⊖ ↑ 1 ↓ ...



red123qwer OP • 3y ago

383 apps counted all the apps that android 7 have,
How can I install 383 apps, there is no space for that many apps.

Plus all the apps that I have installed come from google play, scanned with google trust and I also scan with malwarebytes

↑ 1 ↓ ...



BTCtester • 3y ago • Edited 3y ago

1.2 BTC ended at the Binance client with deposit address bc1q5w6g3tk6lejlkdzk8ly5dlrsxv62n33kugy7ve according to my forensic tools. Go to law enforcement and ask them to freeze the stolen funds at Binance. This goes usually fast but not if you approach the exchange (they don't know if it was a fraud). If they cannot freeze anymore anything then they should get the id because the trade amount requires KYC.

⊖ ↑ 1 ↓ ...



red123qwer OP • 3y ago

I talk with binance and they say

Greetings from Binance security team! We are very sorry to hear about your situation. Upon checking we have found that the funds are in Fixed Float wallet. The funds appear in the blockchain to have been sent to Binance because Fixed Float is a Binance Broker, this means it is another company that has a wallet with Binance for its liquidity and order book. This broker has many users, so we don't know the exact end user who received your stolen funds, we only know the funds were transfer to the Fixed Float hot wallet.

I know fixedfloat is a noKYC exchange own by russians and many bitcoins come and go to the Hydra Market.

⊖ ↑ 1 ↓ ...



BTCtester • 3y ago

Tracing yor transaction leads to more than one Binance address. Did they make this statement as well related to address bc1q5w6g3tk6lejlkdzk8ly5dlrsxv62n33kugy7ve ?

Binance will never help a private person without filing a complaint at police. They cannot know if it was a fraud or a legit business where someone regrets that the bitcoin were spent. Therefore police should approach them. It the funds end up in a binance hot wallet then Binance can freeze the scammers funds.

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

FEB

MAR



06



Log in



2022

2025

2026

About this capture

binance reply that they can do shit. funds was already changed using fixedfloat , what can they frez if they already swap the coin.

fixedfloat is nonKYC exchange

1



BTCtester • 3y ago

As said as a private person you won't get a positive reply, needs to come from authorities. Address bc1q5w6g3tk6lejldzk8ly5dlrsxv62n33kugy7ve has now a balance of 0 but it looks like that this address is reused often so likely there will be funds to freeze soon. Don't give up fast. But up to you.

1



BlankEris • 3y ago

sorry for your loss

i'm assuming your phone, which was past end of life and not receiving security updates had malware. you also had 382 apps any which could of delivered malware to your device.

1



Run-and-Escape • 3y ago

Yeah.. That's not a cold wallet, nor does it even vaguely resemble one. I can't believe someone with 2.4BTC was so careless, incredible..

1



zivac • 3y ago

382 apps... sorry for your loss bro but this one is completely on you

1



red123qwer OP • 3y ago

count every app that the phone app and those are android apps
How can I use 382 apps? there is no storage for that many

1



fxhst329 • 3y ago

such amount should be properly secured. if it went to the user via no-kyc exchange most likely you will not see your funds ever

1

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR 2022

FEB 06 2025

MAR 2026

Log in

About this capture

 LazyXavier • 3y ago

Sorry for your loss! Coinomi is better to avoid. After the spell checker story i did some tests by myself to see the wallet secure. Created test wallets, tried to restore, erase, tested seed phrases created on other wallets... found some bugs: the first is if you restore your seed phrase created on other wallet the coinomi wallet give you another adress and you are lost! Game over. Only if you come back to other app you can go to the funds... after that i stopped and give up. I did not the reversal but if you create a seed on Coinomi probably you will use only on it... one day if it shut down you will be by your own. Avoid also any google software or search, they retain the maximum data as most as they can! Piece and good luck to recover from your loss.

↑ 1 ↓ ...

 r/Bitcoin • 8 yr. ago

BTC-e is back online!



224 upvotes · 88 comments

 r/Bitcoin • 3 yr. ago

How I almost lost all my savings.

362 upvotes · 176 comments

 r/loopringorg • 3 yr. ago

Loopring smart wallet

19 upvotes · 4 comments

 r/Bitcoin • 10 yr. ago

Bye bye 4.7 BTC ... Trojan MSIL Injection

63 upvotes · 271 comments

 r/CryptoCurrency • 3 yr. ago

Got compromised and lost over \$120k in crypto; AMA

2K upvotes · 2.2K comments

 r/Bitcoin • 4 yr. ago

Unpopular opinion: Not your keys not your coins logic doesn't make sense to me. Chances I will die, lose my own keys, get robbed or get screwed over by a friend or family members using multi sig seems like ...

287 upvotes · 287 comments

 r/Bitcoin • 9 days ago

I owe all the bitcoin bros an apology

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

2022

FEB

06

2025

MAR

2026

Log in

?

x

f

t

About this capture

I have just bought my ledger wallet nano s

3 upvotes · 11 comments

 r/Bitcoin • 18 days ago

Bitcoin new ATH \$108xxx!

645 upvotes · 82 comments

 r/Bitcoin • 12 days ago

Do you believe in Bitcoin to the extent that you would put all your savings into it?

658 upvotes · 827 comments

 r/loopringorg • 3 yr. ago

A question about having my wallet on my phone

7 upvotes · 6 comments

 r/synology • 6 yr. ago

Lovin my "Storinator" Definatly choose Synology over Cloud Drives. Next step, play around with DSM and try some fun features....



69 upvotes · 50 comments

 r/cosmosnetwork • 3 yr. ago

ATOM in Crypto.com DeFi wallet

9 upvotes · 21 comments

 r/Bitcoin • 24 days ago

I Found A Forgotten Announcement of BITCOIN V0.1 By Satoshi, 16 Years Ago

522 upvotes · 90 comments

 r/ergonauts • 3 yr. ago

A wallet that works?

9 upvotes · 16 comments

 r/Bitcoin • 3 yr. ago

Lost all my Bitcoin after using Windows activation tool KMSpico

9 upvotes · 70 comments

 r/defi • 3 yr. ago

Best resources/tips on moving ERC20 tokens across chains/intra chain.

Skip to main content

3 captures

2 Mar 2022 - 6 Feb 2025

MAR

2022

FEB

06

2025

MAR

2026

Log in

?

x

f

t

About this capture

I got in at 107k, I hope it drops to \$80k so I can finally sell

730 upvotes · 219 comments

 r/SpellToken • 3 yr. ago

Help...has this happened to anyone? Free crypto showed up in my wallet.

10 upvotes · 17 comments

 r/0xPolygon • 3 yr. ago

screwed---funds stolen from matic mainnet

12 upvotes · 52 comments

 r/Bitcoin • 22 days ago

333 BTC bought and panic sold

1.9K upvotes · 413 comments

 r/Bitcoin • 12 days ago

How many of you doesn't know about Layer 2 for Bitcoin?

325 upvotes · 68 comments

 r/Bitcoin • 28 days ago

I mined bitcoin for a month in 2011, lost most of it to MtGox, cashed out the rest this month

1.3K upvotes · 238 comments

 r/Bitcoin • 1 mo. ago

Do y'all talk with anybody about BTC ?

138 upvotes · 264 comments

TOP POSTS

 Reddit

reReddit: Top posts of March 2, 2022

 Reddit

reReddit: Top posts of March 2022

 Reddit

3 captures

2 Mar 2022 - 6 Feb 2025

Search Bitcoin

MAR 2022

FEB 06 2025

MAR 2026

Log in

Facebook Twitter

About this capture