

Forum: [Hack Forums](#)

Thread: [\\$600 million in Bitcoin Locked.](#)

Therock - December 29, 2025, 10:16 am

A man with over \$600 million in Bitcoin stored on a USB only has two attempts left to unlock it.

Source: <https://x.com/pubity/status/2005672838943093041?s=46>

MadScientist - December 29, 2025, 10:37 am

(Dec 29, 2025 11:16 AM)Therock Wrote: [\[CITE\]](#) A man with over \$600 million in Bitcoin stored on a USB only has two attempts left to unlock it.

Source: <https://x.com/pubity/status/2005672838943093041?s=46>

Remember reading this ages back, so many lost BTC horror stories , like the guy who threw away his old harddrive then wanted to excavate the local dump to find it >.< Probably corrupted by then anyways >.> but billions would be hard to lose while working a 9-5

SUI-3183372 - December 29, 2025, 10:37 am

At this point I'm not convinced Stefan isn't a liar.

A firm approached Stefan in 2023 and showed proof that they could extract the password without risk. They proved it on numerous USB devices under the exact circumstances that Stefan describes. Reporters have sent them encrypted IronKey USB devices and less than 24 hours later this security firm is always capable of sending back the password or the contents of the drive.

However, Stefan refuses to work with them, says he already has someone else working on it for him. Now, more than 2 years later, Stefan is no closer to unlocking the USB stick and everyone else is scratching their heads as to why he won't engage with the security firm that can demonstratively help him. Sounding more and more like Stefan is a phony.

Therock - December 29, 2025, 11:38 am

(Dec 29, 2025 11:37 AM)SUI-3183372 Wrote: [\[CITE\]](#) At this point I'm not convinced Stefan isn't a liar.

A firm approached Stefan in 2023 and showed proof that they could extract the password without risk. They proved it on numerous USB devices under the exact circumstances that Stefan describes. Reporters have sent them encrypted IronKey USB devices and less than 24 hours later this security firm is always capable of sending back the password or the contents of the drive.

However, Stefan refuses to work with them, says he already has someone else working on it for him. Now, more than 2 years later, Stefan is no closer to unlocking the USB stick and everyone else is scratching their heads as to why he won't engage with the security firm that can demonstratively help him. Sounding more and more like Stefan is a phony.

Is it possible to unlock with brute force!

SUI-3183372 - December 29, 2025, 11:55 am

(Dec 29, 2025 12:38 PM)Therock Wrote: [\[CITE\]](#) Is it possible to unlock with brute force!

With the security firm Unciphered, it is possible. They have a method that allows them to attempt trillions of passwords per day, without risk of the device being wiped/encrypted.

Mewtwo - December 29, 2025, 1:49 pm

(Dec 29, 2025 12:55 PM)SUI-3183372 Wrote: [\[CITE\]](#) With the security firm Unciphered, it is possible. They have a method that allows them to attempt trillions of passwords per day, without risk of the device being wiped/encrypted.

Either that or there's a poor algorithm built in. I think there was an article about how the password was retrieved simply on the timestamp and some other thing of the computer. If I could find that article, would be a really interesting read.

SUI-3183372 - December 29, 2025, 2:56 pm

(Dec 29, 2025 02:49 PM)Mewtwo Wrote: [\[CITE\]](#) Either that or there's a poor algorithm built in. I think there was an article about how the password was retrieved simply on the timestamp and some other thing of the computer. If I could find that article, would be a really interesting read.

This is from the Wired interview with Unciphered:

<https://www.wired.com/story/unciphered-ironkey-password-cracking-bitcoin/> (Paywalled)

200 trillion attempts sounds like straight up blind bruteforcing to me, unless maybe you're talking about another group working on this.

Mewtwo - December 29, 2025, 9:39 pm

(Dec 29, 2025 03:56 PM)SUI-3183372 Wrote: [\[CITE\]](#) This is from the Wired interview with Unciphered:

<https://www.wired.com/story/unciphered-ironkey-password-cracking-bitcoin/> (Paywalled)

200 trillion attempts sounds like straight up blind bruteforcing to me, unless maybe you're talking about another group working on this.

<https://arstechnica.com/information-technology/2024/05/researchers-crack-11-year-old-password-rec-over-3-million-in-bitcoin/>

It was this one.

They were able to figure out the password based off the time and date of the computer, along with knowing how long the password was if the owner knew it. It was Roboform password manager that had a weak random flaw

Clonazepam - January 3, 2026, 9:02 am

(Dec 29, 2025 11:37 AM)SUI-3183372 Wrote: [\[CITE\]](#) At this point I'm not convinced Stefan isn't a liar.

A firm approached Stefan in 2023 and showed proof that they could extract the password without risk. They proved it on numerous USB devices under the exact circumstances that Stefan describes. Reporters have sent them encrypted IronKey USB devices and less than 24 hours later this security firm is always capable of sending back the password or the contents of the drive.

However, Stefan refuses to work with them, says he already has someone else working on it for him. Now, more than 2 years later, Stefan is no closer to unlocking the USB stick and everyone else is scratching their heads as to why he won't engage with the security firm that can demonstratively help him. Sounding more and more like Stefan is a phony.

Think it's a made up story.

