

Forum:[Hack Forums](#)

Thread: [XMR wallet got drained](#)

wuistberkin - January 21, 2026, 9:54 pm

I'm starting to think hackers are running code to generate random seed while checking to see if it hold funds.

I don't believe my wallet seed phrase got exposed but instead the above happened.

A few months ago i generated a XRP wallet address. The minute i sent funds to that wallet it automatically got drained.

I think seed generation for these coins is not truly random if done on a regular computer, which in turn can be easily guessed

Artisan - January 21, 2026, 11:32 pm

You could have been infected with a stealer.

Mewtwo - January 22, 2026, 12:12 am

(Jan 21, 2026 10:54 PM)wuistberkin Wrote: [\[CITE\]](#) I'm starting to think hackers are running code to generate random seed while checking to see if it hold funds.

I don't believe my wallet seed phrase got exposed but instead the above happened.

A few months ago i generated a XRP wallet address. The minute i sent funds to that wallet it automatically got drained.

I think seed generation for these coins is not truly random if done on a regular computer, which in turn can be easily guessed

100% your computer has to be infected. Either that or you're using a fake software that is stealing your private / seeds.

caspperr - January 22, 2026, 4:30 am

That's not how it works. Randomly generating seed phrases and finding funded wallets isn't realistically possible the number of combinations is astronomical. If a wallet gets drained instantly, it means the seed/private key was exposed somehow (malware, compromised generator, reused seed, etc.), not that someone guessed it.

wuistberkin - January 22, 2026, 5:11 am

(Jan 22, 2026 05:30 AM)MKacc Wrote: [\[CITE\]](#) That's not how it works. Randomly generating seed phrases and finding funded wallets isn't realistically possible the number of combinations is astronomical. If a wallet gets drained instantly, it means the seed/private key was exposed somehow (malware, compromised generator, reused seed, etc.), not that someone guessed it.

it's not truly random if generated of a regular computer... theres no entropy like a true hardware device that also uses sounds etc. I'm also using a macbook ... macbooks are extremely hard to keylog or virus.

RangoWorld - January 22, 2026, 6:52 am

Nah. That sounds like a stealer was awaiting. Infected. Your machine is either compromised or your

browser or the method you used to generate the wallet. Somewhere in between the process something was compromised. Not the wallet phrase necessarily but something that would've allowed the hacker to drain the wallet.

If cracking phrases or secret key was that easy then they would've already gotten their hands to 8-9 digit wallets. \$\$\$

? sentient ? - January 22, 2026, 7:33 am

(Jan 22, 2026 06:11 AM)wuiatberkin Wrote: [\[CITE\]](#) it's not truly random if generated of a regular computer... there's no entropy like a true hardware device that also uses sounds etc. I'm also using a macbook ... macbooks are extremely hard to keylog or virus.

If no seed phrase is ever truly random then thank you so much for your kind warning, I will move all my crypto to my bank.

Regarding your loss, I'm so sorry. But with this realization, you should be able to easily recover what you lost and then some.

I don't get what you mean about the macbook, but maybe that's just because I'm no encryption-Senpai like you.

May the Lord guide your steps and light your path.

You know what you need to do.

Always Sad - January 22, 2026, 8:18 am

Don't click on any types of links you were sent....

That's how you get drained easily..

I have "Pocket Universe" add on on Chrome it protects ETH, USDC and NFTS.

Omniscient - January 22, 2026, 1:11 pm

XRP or XMR? Your thread title says XMR but your post says XRP.

And which wallet do you use? And do you also use the wallet (synced?) with your mobile?

Almost certainly you got hit with a drainer. Oh, and did your wallet have a password?

SUI-3183372 - January 22, 2026, 2:03 pm

ITT a bunch of people who don't realize the word lists used for seed phrases contain a finite number of predefined words, and that every private key and/or seed phrase for every wallet in existence is already known. The only reason why every wallet in existence isn't robbed is because the number of wallets that can exist is a staggering number, and nobody can check all of them (not even with super computers). Want an example? <https://keys.lol> lists every single private key to every single bitcoin wallet that has ever existed or will ever exist. It also lists how much BTC each wallet holds, and how many transactions each wallet has engaged in. You will never find a wallet with funds in it on this list (other than a few edge cases towards the start and end of the list, those wallets are inaccessible).

The most commonly used word list is known as BIP-39 (due to it being introduced in the 39th Bitcoin Improvement Proposal). BIP-39 contains just 2048 words. That means for every word in your seed phrase, there's just 2048 options for what it can be. That may sound frighteningly small at face value, but when you realize the total number of potential phrases is 2^{128} , which equals

340,282,366,920,938,463,463,374,607,431,768,211,456, it becomes evident that there's no real risk of collision or someone otherwise stumbling across your wallet by generating seed phrases randomly.

Conclusion: The approach that OP describes is perfectly valid, assuming you like wasting your time. Every private key for every wallet on every network is theoretically known. However, finding a wallet with funds on it within this list is like finding a singular needle in a billion^billion haystacks.

30,000,000 to 35,000,000 Bitcoin wallets hold at least \$10.
Chance to collide with a specific crypto wallet (targeted attack): 1 / 340,282,366,920,938,463,463,374,607,431,768,211,456
Chance to collide with any wallet holding >\$10 in value: 1 / 11,342,745,560,000,000,000,000,000,000 (approximated)
Chance to win the \$1,000,000,000 mega millions lottery: 1 / 290,500,000

You have a better shot at winning the mega millions lottery literally 39,062,500,000,000,000,000,000 times before you'd find a crypto wallet with \$10+ in it.

Edit: math is hard

wuistberkin - January 25, 2026, 10:38 am

(Jan 22, 2026 02:11 PM)Omniscient Wrote: [\[CITE\]](#) XRP or XMR? Your thread title says XMR but your post says XRP.

And which wallet do you use? And do you also use the wallet (synced?) with your mobile?

Almost certainly you got hit with a drainer. Oh, and did your wallet have a password?
Can you explain more what a drainer is?

For my XMR i was using the official monero gui wallet for macbook <https://www.getmonero.org/>

My funds was safe for the past year then suddenly got drained. Funny thing is i've continued to use this wallet just created a new seed and that current wallet hasn't been drained so i'm thinking maybe xmrwallet.com hacked me? I used to use their online hot wallet i'm thinking they stored my seed.

For my XRP it was definitely my seed already being exposed. I used <https://github.com/billian/qrcash-paper-wallet> to generate a seed, the minute i sent funds to that address the funds was automatically sent out.

(Jan 22, 2026 03:03 PM)SUI-3183372 Wrote: [\[CITE\]](#) ITT a bunch of people who don't realize the word lists used for seed phrases contain a finite number of predefined words, and that every private key and/or seed phrase for every wallet in existence is already known. The only reason why every wallet in existence isn't robbed is because the number of wallets that can exist is a staggering number, and nobody can check all of them (not even with super computers). Want an example? <https://keys.lol> lists every single private key to every single bitcoin wallet that has ever existed or will ever exist. It also lists how much BTC each wallet holds, and how many transactions each wallet has engaged in. You will never find a wallet with funds in it on this list (other than a few edge cases towards the start and end of the list, those wallets are inaccessible).

The most commonly used word list is known as BIP-39 (due to it being introduced in the 39th Bitcoin Improvement Proposal). BIP-39 contains just 2048 words. That means for every word in your seed phrase, there's just 2048 options for what it can be. That may sound frighteningly small at face value, but when you realize the total number of potential phrases is 2^{128} , which equals 340,282,366,920,938,463,463,374,607,431,768,211,456, it becomes evident that there's no real risk

of collision or someone otherwise stumbling across your wallet by generating seed phrases randomly.

Conclusion: The approach that OP describes is perfectly valid, assuming you like wasting your time. Every private key for every wallet on every network is theoretically known. However, finding a wallet with funds on it within this list is like finding a singular needle in a billion^billion haystacks.

30,000,000 to 35,000,000 Bitcoin wallets hold at least \$10.

Chance to collide with a specific crypto wallet (targeted attack): $1 /$

340,282,366,920,938,463,463,374,607,431,768,211,456

Chance to collide with any wallet holding >\$10 in value: $1 /$

11,342,745,560,000,000,000,000,000,000 (approximated)

Chance to win the \$1,000,000,000 mega millions lottery: $1 / 290,500,000$

You have a better shot at winning the mega millions lottery literally

39,062,500,000,000,000,000,000 times before you'd find a crypto wallet with \$10+ in it.

Edit: math is hard Your missing my point. True randomness is if you buy a trezor then yes, thats truly random. If you do the BIP 39 on a computer it's still predictable.

Response from Gemini.

Question - when generating a seed on a computer using bip 39 is it truly random

The short answer is: No, but it's "random enough" that it doesn't matter.

In the world of computing, there is a big difference between true randomness and pseudorandomness. When you generate a BIP-39 seed phrase on a standard computer, you are almost certainly using the latter.

1. The "Pseudo" Problem

Computers are logic machines designed to be predictable. If you give a computer the same input and the same instructions, it should always produce the same output. This is the opposite of randomness.

Omniscient - January 25, 2026, 10:43 am

Did you have passwords on your wallets? Because realistically that's likely how they got you. The PW encrypts the seed phrase in the wallet. Thus making seed extraction more difficult. If you have no PW then a drainer will read the seeds on your computer and start to drain funds.

AI Quote: A crypto drainer that targets an app or desktop program is a type of malicious software disguised as a legitimate wallet, trading tool, miner, game, or "crypto utility." When a user installs and runs it, the program secretly steals sensitive information such as private keys, seed phrases, wallet files, or authentication tokens. Some drainers also monitor the clipboard to replace copied wallet addresses with the attacker's address, or inject code that redirects transactions without the user realizing it.

For someone new to crypto, the important takeaway is that these drainers don't need you to click a website or approve anything. The damage happens because the software itself is untrusted. Once a private key or wallet file is stolen, the attacker can empty the wallet remotely, and there is no way to reverse it. This is why downloading crypto-related software only from official sources, avoiding cracked or "free" tools, and keeping wallets on dedicated, clean devices is critical for staying safe.

Three - January 25, 2026, 12:29 pm

(Jan 25, 2026 11:38 AM)wuistberkin Wrote: [\[CITE\]](#) xmrwallet.com

You actually answered that yourself. There are many reports of fraud. If the seed you're using in your monero gui wallet is the same, then the source of the problem is clear.

(Jan 25, 2026 11:38 AM)wuistberkin Wrote: [\[CITE\]](#) Your missing my point. True randomness is if you buy a trezor then yes, thats truly random. If you do the BIP 39 on a computer it's still predictable.

The situation is different with hardware wallets. However, the probability of correctly predicting the BIP39 seed on a computer is even lower than winning the lottery multiple times in a row.

Mewtwo - January 25, 2026, 1:14 pm

(Jan 25, 2026 11:38 AM)wuistberkin Wrote: [\[CITE\]](#) Can you explain more what a drainer is?

For my XMR i was using the official monero gui wallet for macbook <https://www.getmonero.org/>

My funds was safe for the past year then suddenly got drained. Funny thing is i've continued to use this wallet just created a new seed and that current wallet hasn't been drained so i'm thinking maybe xmrwallet.com hacked me? I used to use their online hot wallet i'm thinking they stored my seed.

For my XRP it was definitely my seed already being exposed. I used <https://github.com/billian/qrcash-paper-wallet> to generate a seed, the minute i sent funds to that address the funds was automatically sent out.

Your missing my point. True randomness is if you buy a trezor then yes, thats truly random. If you do the BIP 39 on a computer it's still predictable.

Response from Gemini.

Question - when generating a seed on a computer using bip 39 is it truly random

The short answer is: No, but it's "random enough" that it doesn't matter.

In the world of computing, there is a big difference between true randomness and pseudorandomness. When you generate a BIP-39 seed phrase on a standard computer, you are almost certainly using the latter.

1. The "Pseudo" Problem

Computers are logic machines designed to be predictable. If you give a computer the same input and the same instructions, it should always produce the same output. This is the opposite of randomness.

It's more than likely you clicked a phishing version or a homograph attack of iancoleman's BIP39. If you used Bing (Microsoft's search), you're TOTALLY screwed because there's so many scam websites that are promoted on the top.

The only other way you've been attacked is using an outdated browser, or a compromised one.

Otherwise, the source code is here: <https://github.com/iancoleman/bip39>

There is true mathematic randomness on his software.

AI Quote:

Short answer: it's as random as your operating system's cryptographic RNG — which is about as good as it gets in consumer software.

Here's the precise breakdown ?

?

What randomness source does it use?

The Ian Coleman BIP-39 generator uses:

`window.crypto.getRandomValues()`

That API pulls entropy from the OS CSPRNG:

- Windows -> CryptGenRandom / BCrypt
- macOS / iOS -> /dev/random-backed system RNG
- Linux / Android -> kernel entropy pool

This is the same class of randomness used for:

- HTTPS keys
- Password managers
- Hardware wallets (at the OS level)
- Secure session tokens

No `Math.random()`. No time-based seeds. No PRNG shortcuts.

?

How much entropy is actually generated?

Mnemonic Entropy bits Security level
12 words 128 bits $\sim 3.4 \times 10^{38}$ possibilities
15 words 160 bits astronomically large
18 words 192 bits overkill
21 words 224 bits absurd
24 words 256 bits effectively unbreakable

To put 128 bits in perspective:

- Brute-forcing it would take longer than the age of the universe
- Even with all computers on Earth combined

?

Is the randomness biased or predictable?

No, assuming:

- Modern browser
- Normal OS
- No malware
- Not a broken VM snapshot

The BIP-39 checksum step does not reduce security — it only ensures typo detection.

?

What can actually make it less random?

These are the real risks (not the code):

1. Typing your own entropy
 - Humans are terrible RNGs
2. Compromised OS or browser
 - Malware > any crypto algorithm
3. Copying seeds while online
4. Using a modified or fake clone of the site
5. Running inside a bad VM snapshot (same entropy reused)

The generator itself is not the weak link.

?

Bottom line

- Cryptographically strong
- Industry-standard
- Equivalent randomness to hardware wallets
- Safe if your environment is safe

If you want, I can:

- Walk you through verifying the RNG call in the source code line-by-line
- Tell you whether offline HTML vs hardware wallet is safer for your exact setup
- Explain how entropy failures actually happen in real-world wallet losses

Just say the word.

Omniscient - January 25, 2026, 4:15 pm

(Jan 25, 2026 02:14 PM)Mewtwo Wrote: [\[CITE\]](#) Otherwise, the source code is here:

<https://github.com/iancoleman/bip39>

There is true mathematic randomness on his software.

<https://hackforums.net/tools.php?action=bip39>

HF runs that script in our Hacking Tools. It's purely client side, HF does no logging or scripting on our server side. I use it myself if I need to create a seed.