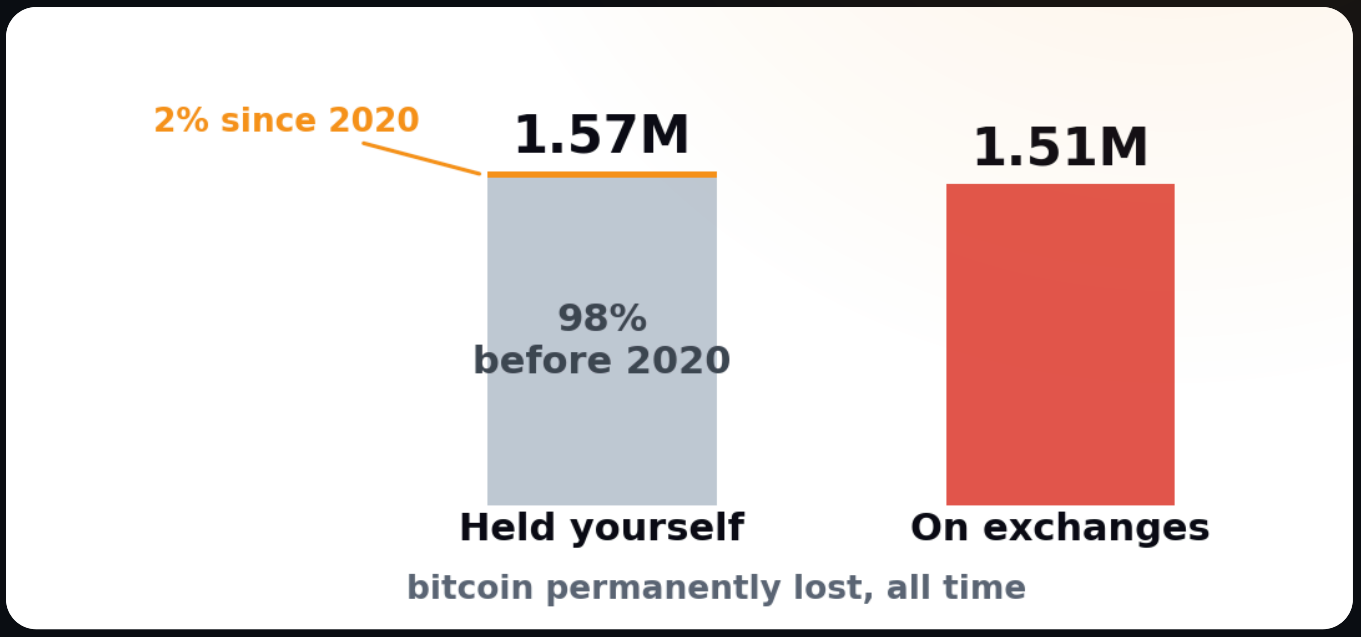
# THE STORAGE SAFETY CHECKLIST

A wallet that was never online just lost more than $130 million.

What actually broke, how to check your own device tonight, and how to hold Bitcoin so that no single failure can ever take all of it.




**$130M+**
taken from offline wallets in five days

**5 years**
the bug sat there unnoticed

**8 steps**
in the checklist at the back

Educational, not financial advice. Every number in here traces to a primary source, and where the data does not exist I say so instead of guessing.

Bitcoin Jae
@bitcoin.daily

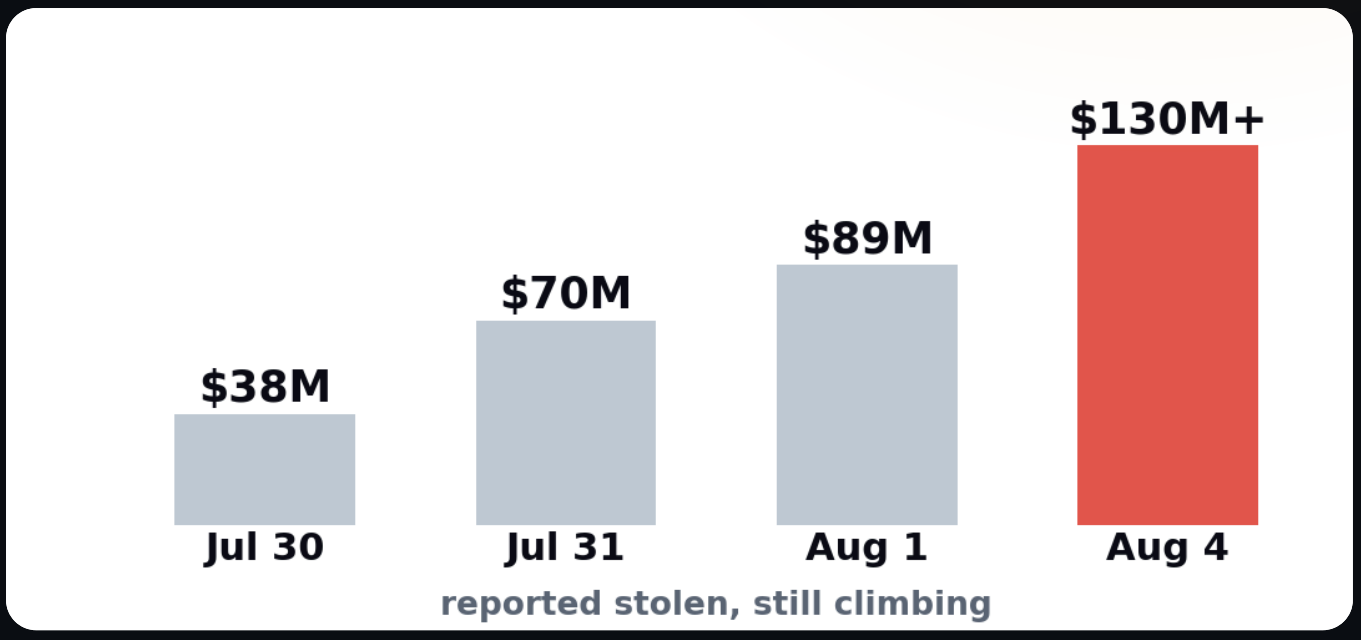
WHAT ACTUALLY HAPPENED

# THE LOCK WAS FINE. THE FACTORY WAS NOT.

A hardware wallet keeps your Bitcoin safe with a secret recovery phrase. That phrase has to be built out of pure randomness. If the randomness is real, nobody on earth can guess your phrase, even with every computer ever made.

In March 2021, Coldcard shipped firmware version 4.0.0. One line in it told the device to stop using its dedicated randomness chip and fall back to software randomness, seeded with information that was not secret.

**The phrases it produced were guessable.** Instead of the 128 bits of randomness a phrase is supposed to carry, affected devices produced around 72. That gap sounds small. It is not. It is the difference between impossible and a weekend of computing.




Nobody broke into a house. No malware, no phishing, no stolen device. Attackers rebuilt the phrases from scratch and swept the coins straight off the blockchain. Being offline was never the thing that failed.

*Loss totals reported by Galaxy Research via CoinDesk, Fortune and TechCrunch, July 30 to August 4, 2026. The figure was still climbing at the time of writing.*

CHECK YOUR OWN DEVICE

# ARE YOU AFFECTED?

Most of the coverage got this part wrong and told people that only the Mk3 was at risk. Coinkite's own advisory says otherwise. Here is the actual list.

| DEVICE | AFFECTED FIRMWARE | FIXED IN |
|---|---|---|
| **Mk2 and Mk3** | 4.0.1 through 4.1.9 | 4.2.0 or later |
| **Mk4 and Mk5** | Anything before 5.6.0 | 5.6.0 or later |
| **Q** | Anything before 1.5.0Q | 1.5.0Q or later |
| **Mk4 and Mk5 (Edge)** | Anything before 6.6.0X | 6.6.0X or later |
| **Q (Edge)** | Anything before 6.6.0QX | 6.6.0QX or later |
| **TAPSIGNER, OPENDIME, SATSCARD** | Not affected | No action needed |

*Source, Coinkite security advisory. What matters is the firmware version your phrase was CREATED on, not the version running today.*

**Two groups came out of this fine.** Anyone who added 50 or more of their own private dice rolls when setting the wallet up, because those rolls put real randomness back into the phrase. And most people running a strong, unique passphrase on top of their phrase.

READ THIS TWICE

**The single most important line in this guide. Updating your firmware does NOT fix an already weak phrase. A phrase that was guessable when it was created stays guessable forever. You need a brand new one.**

This trips people up, so it is worth saying plainly. The version running on your device today tells you nothing about whether you are safe. What matters is the version that was running on the day your recovery phrase was first created. The weakness was baked into the phrase at birth.

**If you cannot remember which firmware you set it up on, treat it as exposed.** Migrating when you did not need to costs you an afternoon and a transaction fee. Not migrating when you did need to costs you everything.

IF YOU ARE AFFECTED

# THE MIGRATION, IN ORDER

These are Coinkite's own steps, in their order. Do not skip the test transaction and do not destroy the old backup early. More coins are lost to botched migrations than to attackers.

1. Confirm the fixed firmware version is actually installed on the device.
2. Generate a brand new seed phrase on the updated device.
3. Write down the new backup and verify it before you deposit anything.
4. Verify a fresh receive address on the device screen itself, not on your computer.
5. Send one small test transaction and confirm the new wallet works.
6. Only then move the remaining funds across.
7. Keep the old backup until the migration is finished and confirmed.

**The four ways people lose coins during a migration like this one.** Every one of these is more common than the exploit that started it.

| THE MISTAKE | WHY IT COSTS YOU |
|---|---|
| **Typing the phrase into a computer or phone** | That is the one thing the device exists to prevent. A phrase typed into a connected machine is a phrase that has left the device. |
| **Photographing the backup** | Photos sync to the cloud automatically. Your backup is now on somebody else's server. |
| **Destroying the old backup too early** | If the new setup has a problem you have no way back. Keep it until the last coin has moved and confirmed. |
| **Moving everything in one transaction** | You find out the new wallet is wrong after the funds are already in it. The small test send exists for this. |

*If your coins are already gone, the sweep happened on-chain and cannot be reversed. Report it, keep your records, and be extremely careful with anyone who contacts you offering to recover funds. Recovery scams follow every hack like this one.*

THE ARGUMENT THIS STARTED

# SAME SIZE, VERY DIFFERENT STORY

Within days the hack became ammunition. An analyst posted two totals from River's 2025 custody report. The founder of Binance concluded that exchanges are statistically safer than holding it yourself.

**1.57M**
coins lost in self-custody, all time

**1.51M**
coins lost on exchanges, all time

**98%**
of the self-custody losses happened before 2020

That third number is in the same report, and it changes everything. Almost all self-custody losses are ancient. They are coins from an era when Bitcoin cost pennies, sitting on hard drives that got wiped, thrown out, or forgotten. That is a story about 2011, not about whether your wallet is safe today.

**The exchange column did not stop.** River records more than 100,000 coins lost in 2022 alone at platforms paying yield, plus around $2.6 billion lost to insider theft since 2020.

There is a second problem with putting those totals side by side. Most Bitcoin has always been held by people themselves, across far more coins and far more years than anything parked on an exchange. A much bigger pile will lose more coins in total even when it is safer per coin. Comparing raw totals without comparing the size of each pile is not a fair fight.

**Now the part that cuts the other way.** He also made a point that is fair and that most people replying to him ignored. Exchange hacks are loud and get reported. Losses in self-custody are quiet, personal, and often never reported at all. So the self-custody number is probably an undercount, and nobody can tell you by how much.

He is also right that a few dead exchanges drag the whole exchange column down, and that some exchanges have covered users out of their own pocket after a hack. And his actual conclusion was that a balanced approach is probably best, which is closer to the truth than the headline his post turned into.

*River estimates lost coins using on-chain heuristics and states it cannot cleanly separate self-custody losses. There is no published pre-2020 and post-2020 split for the exchange column, so this guide does not claim one. Both columns are estimates, and both are probably low.*

THE PART NOBODY ARGUED ABOUT

# EVERY METHOD HAS ONE WAY IT DIES

The whole argument was about which single basket is safest. Coldcard is the proof that this is the wrong question. One line of code reached every owner of one brand on the same day, no matter how carefully any of them had stored it.

| WHERE IT SITS | WHAT CAN TAKE IT ALL | WHAT IT SURVIVES |
|---|---|---|
| **On an exchange** | Company failure, insider theft, freeze or seizure, a hack | Your own mistakes, fire, a lost device |
| **One hardware wallet** | A firmware or supply-chain bug, a lost or destroyed backup, theft, you dying without a plan | An exchange collapsing |
| **Two wallets, same brand** | The same firmware bug, hitting both at once | One device breaking or being lost |
| **Two wallets, different brands** | Your own backup mistakes | Any single vendor's bug |
| **Multisig, keys apart** | Losing track of the setup itself | Any one key being lost or stolen |

*Read the middle column. That is your single point of failure, and it is different for every row.*

Notice that the last two rows do not appear anywhere in the argument that started this. They are not a compromise between the two sides. They are the answer to a better question.

**What that looks like in practice.** Somebody holding one hardware wallet with everything on it moves to holding most of it on that wallet and the rest on a device from a different maker, with the two backups stored in two different buildings. Nothing clever happened. But there is now no single bug, fire, or burglary that takes all of it.

THE TRADE-OFF

**Be honest with yourself about the cost. Spreading it out means more backups to keep track of, more setups to remember, and more ways to confuse your future self. That is a real price. Losing everything to one bug is a bigger one.**

THE CHECKLIST

# SPREAD IT, THEN PROVE IT

None of this requires being technical. It requires refusing to let one thing hold everything.

1. Split across at least two independent methods. Not two of the same device from the same maker, because that is one point of failure wearing a disguise.
2. Add your own randomness when you create a phrase. The dice-roll users are the ones who walked away from this untouched.
3. Add a passphrase on top of your recovery phrase, and back that up separately from the phrase itself.
4. Test your backup by restoring it onto a device BEFORE you trust it with real money. An untested backup is a guess.
5. Keep backups in separate physical places. Fire, flood and burglary are boring, and they take far more coins than exploits do.
6. Always verify the receive address on the device's own screen. Your computer can lie to you. The device screen is the point of the device.
7. Write down who gets access if something happens to you. A huge share of that 1.57 million was not stolen. It was simply lost.
8. Re-check your setup when firmware updates land. This exact bug sat quietly for five years.

THE WHOLE GUIDE IN ONE LINE

**The people who survived this week were not the ones who picked the right brand. They were the ones who never let a single thing hold all of it.**

BITCOIN DAILY

# COME FIND ME

This is the kind of breakdown I do every day. The hype brings the noise. I bring the data.

**BD** **bitcoin-daily.com**
Every free guide, the live cycle charts, and the daily blog, all in one place
bitcoin-daily.com/guides

**IG** **Instagram**
The live read every morning, daily charts, and the honest call on the market
@bitcoin.daily

**YT** **YouTube**
Deep breakdowns like this one, every claim checked against the data
bitcoindailytv

**X** **X / Twitter**
More data threads like this one
@BitcoinxDaily

**Bitcoin Jae**
@bitcoin.daily · Educational, not financial advice