

Harmony

Security Public Service Announcement



Wallet Security and Your Assets

Wallet Security | a Public Service Announcement

by Elias Bou Zeid, April 2022

TLDR: Browser extension wallets are only as strong as the underlying Operating System and security practices of the user. Software wallets across the entire crypto community can be and are compromised through various technological and social means; the Harmony Chrome extension wallet is no exception. Control of your funds means control of your private key - this means **using a hardware wallet, removing unsupported wallets from your computer, and using high complexity passwords**, especially if you cannot purchase a hardware wallet.



Critical Message: The Harmony Chrome Extension wallet will be unlisted starting **May 2nd, 2022**. In addition, the Harmony team has recently observed an uptick in wallet compromises. **If your funds have been stored in this Chrome Extension wallet, please transfer your assets to a new wallet such as a Ledger Nano or MetaMask as soon as possible.** We strongly recommend using a **brand new** account without reusing your existing private key for maximum security and peace of mind.

With the ever-increasing headlines of today's financial crisis around the world, many have turned to cryptocurrency as an alternate avenue to finance. However, with all new and innovative tech comes unintended caveats and weaknesses. In the case of cryptocurrency, it is security. This is not to say that the technology of blockchain itself is not secure, but instead, it is the ability for individuals to keep themselves

safe from bad actors. As a result, we've witnessed a slew of crypto hacks, or otherwise vulnerabilities, that lead to compromises of individual and community wallets across the entire cryptocurrency space.

To help educate the community, this article aims to provide some understanding of where these vulnerabilities lie and how better to protect yourself against them.

Cryptocurrency Wallet Compromises



For a more comprehensive list, see: [REKT Database](#) | [DEFIYIELD](#)

Hacked wallets and stolen crypto assets are unfortunately prevalent in this sector. The cryptocurrency community has seen report after report of stolen assets from various wallets, primarily through browser extension wallets. Offenders use a variety of methods to compromise a wallet and illegally access your tokens.

From clipboard hacks and a number of other types of malware, to social engineering, phishing and spoofing; browser extensions are only as strong as your computer's security, and your wallet (regardless of its location) is only as strong as a person's security practices.

- <https://metamask.zendesk.com/hc/en-us/articles/360052511372-i-ve-been-hacked-scammed-unauthorized-transactions-on-my-account->
- <https://medium.com/coinmonks/how-your-metamask-got-hacked-probably-795abca4534a>
- <https://medium.com/coinmonks/tricks-hackers-use-to-steal-crypto-from-people-on-metamask-2e350039410c>

Whether you're storing your crypto assets on Metamask or the now deprecated Harmony Chrome extension wallet, your funds and private key are always vulnerable to software and social exploits.

Notable Wallet Compromise in the Harmony Community:

- Harmony [Community member](#) hacked for 4.7 Million [Jewel](#) worth an estimated \$49,961,000 at time of theft.

Broader Crypto Community Hacks:

https://www.reddit.com/r/ethereum/comments/se017w/lost_17000_of_eth_due_to_hacked_metamask_walle

<https://www.shellypalmer.com/2021/12/my-metamask-eth-wallet-was-hacked/>

https://www.reddit.com/r/Metamask/comments/pjbelm/wallet_got_hacked_emptied_unsure_how_nft_please/

<https://t4techblog.com/got-hacked-on-metamask-these-could-be-reasons/>



Unfortunately, these hacks are just a small glimpse into what is currently happening across Web3. **Most recently, there have been Zero-Day vulnerabilities discovered for Chrome & Edge browsers**, which essentially means that hackers are privy to and exploit weak spots in a software's code that the developers themselves are unaware of.

Recent Harmony ONE Wallet Compromises



[Details about Harmony Wallet Attacks](#)

Recently, Harmony has had numerous reports from the community of compromised Chrome Extension ONE wallets. As of this current moment, Harmony is still investigating these incidents (details below) and will share a report with the community once investigations are complete.

Status of the Investigations

- Harmony's cyber security team has performed thorough forensic investigations while also retaining the help of reputable security firms and multiple white-hat hackers in an attempt to determine root cause and assist in identifying the suspect.
- Major exchanges have been contacted to be made aware of the situation and provided the hackers wallet addresses. We will continue to expand these efforts and cast a wide net.
- Harmony's cyber team documented a detailed report which has been provided to the authorities describing the timeline of events, and forensic information they have gathered.
- Local and national authorities have been contacted. Our team has met with national officials to provide them with our detailed report, and to work together in full cooperation.

Wallet Investigation Status:

The security firms and white hat hackers we partnered with have yet to find concrete proof of a critical vulnerability or root cause in the Harmony Chrome extension wallet itself.

However, as many of you are aware, there have been two recent and critical vulnerabilities in the Chrome web browser which can directly lead to a compromised private key.

See below for more:

- <https://thehackernews.com/2022/04/google-releases-urgent-chrome-update-to.html>
- <https://www.tomsguide.com/news/update-chrome-now-urgent-zero-day-flaw-under-attack>
- <https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/03/update-now-google-releases-emergency-patch-for-chrome-zero-day-used-in-the-wild/>

Due to the recent uptick in reported thefts, and the sunset status of the wallet, we are setting a date for the removal of **Harmony Chrome extension wallet** from the Chrome web store. Existing installs will continue

working with sunset disclaimers but users are suggested to purchase a hardware wallet or create a new Metamask wallet and transfer funds to the new address.

The extension will be unlisted from the Chrome web store on May 2nd 2022.

To reiterate, security firms and white-hat hackers we partnered with have yet to find concrete proof of a critical vulnerability in the Harmony Chrome extension wallet, but we still feel this decision is in the best interest of the community.



Harmony suggests to store your crypto assets on a the most secure storage method, a hardware wallet. However, if you cannot use a hardware wallet, ensure that your software wallet is secured using a complex password with a minimum of 14 characters comprised of numbers, symbols, upper and lowercase characters.

Note: The security of your extension wallet is only as strong as the Operating System and browser on which it resides, and is always at risk of compromise via social engineering and phishing.

Number of Characters	Numbers only	Upper or Lower case letters	Upper or Lower case letters mixed	Numbers, Upper & Lower case letters	Numbers, Upper & Lower case letters, Symbols
3	instantly	Instantly	Instantly	instantly	instantly
4	Instantly	Instantly	Instantly	Instantly	instantly
5	instantly	instantly	instantly	3 secs	10 secs
6	instantly	instantly	8 secs	3 mins	13 mins
7	instantly	instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1 qt years

Security Overview & Suggestions

Private Keys



In-depth information on [Public Key Cryptography](#).

The first time you buy cryptocurrency and create a wallet, you are issued two keys: a **public key** and a **private key**. A **public key** works like an email address that can be shared with others.

The private key, on the other hand, is extremely sensitive information and should NEVER be shared with anyone. In most cases, a private key is a string of letters and numbers.

You can think of the private key as a complex password that unlocks the vault that holds your funds. As long as you and only you have access to your private key, your funds are safe and can be managed anywhere globally by using a hardware wallet.

The Challenges With Private Keys

Platform Security

Sure, private keys are what make a blockchain safe but, unfortunately, the machines on which we store them sometimes are not safe. On a desktop (especially Windows) applications have no isolation, which means one application can read another, thus making it easier for malware to steal data across applications. Multiple types of malware are known to steal browser extension wallet key-stores ([oski](#)). Mobile OSs are much better at this by isolating applications at the directory level, and preventing unknown applications from running.

Desktops (especially Windows) lack trusted platform modules (TPMs). TPMs are essential to store the private key safely to prevent unauthorized access, and on-chip (trusted zone) signing so that the private key is never loaded into memory. Mobile wallets (iOS) already provide this feature which is generally known as *keychains*. Hardware wallets are built around TPMs.

Forms of Private Key Storage & Their Security Ratings

Insecure

- **Desktop & Chrome Extension Wallets:** No TPM (Trusted Platform Module), no app isolation.

Secure

- **Mobile wallets (iOS):** TPM or Secure Enclave, app isolation.

Very Secure

- **Hardware wallets (Ledger Nano S & Nano X):** TPM, no external applications or network connection “cold storage”.

Seed Phrase

Seed phrases are derived from your private key. Access to a seed phrase will also provide access to its corresponding private key. The biggest challenge is that you never know **when**, or **if** it has been compromised. Bad practice around seed phrase storage compounds this problem.

Copies of the user's seed phrase may be on a plain text file, note app, google/dropbox drive, or even email. Users sometimes use the exact seed phrase on multiple machines and wallets. If these storage mediums are compromised, the user's private key is at risk of being exposed.



If you have a hardware or software wallet, you should NEVER store the seed phrase in a notes app or any other app-based or unencrypted medium.

Suggestion: How to Store Your Seed Phrase

- In something that you control *who* has access to it, preferably in an accessible place where you can check on the seed regularly. Somewhere permanent that won't be moved without you knowing.
- DO NOT store on any medium that is connected to the internet.
- On paper & pencil in two different secure locations. Ensure it's stored in something durable and safe from natural elements; a memorable location, unlikely to be forgotten by you.
- On a steel or titanium cold storage solution such as the Ledger Billfodl.
- Split the seed phrase in different places such that the 1st location has words 1-16 and the 2nd location has 8-24, or something similar.
- Memorize it.
- Encrypted SD card using AxCrypt or VeraCrypt.

Most Secure Wallet: The Hardware Wallet

For the ultimate protection of your ONE coins, Harmony strongly recommends using a hardware wallet such as the Ledger Nano S & Nano X.

The Nano S and X are hardware wallets created by Ledger. A hardware wallet stores the private keys to Harmony tokens on a separate device, making it much harder for malicious parties to steal them. In fact, the private keys never leave the Nano wallet itself, so they will remain secure even if the device is connected to a compromised computer. As long as you follow best practices when using your Nano, it is virtually impossible for an attacker to steal your funds.

Still Using a Browser Extension Wallet?

If you don't think that a hardware wallet is something you will use, Harmony suggests the following actions to safeguard your assets:

1. Create a new wallet via Metamask every **6 months** and migrate your ONE assets to it.
2. Use a complex password consisting of a **minimum** of 14 characters, with symbols, numbers, lowercase and uppercase letters.
3. Spread your assets across different Metamask wallets.

4. Uninstall unsupported browser extension wallets as they are no longer kept up-to-date from a security perspective. Leaving them installed means its private keys are still on your computer.

Final Thoughts

In conclusion, cryptocurrencies are rapidly gaining popularity, and unfortunately, there are bad actors waiting to take advantage of users. One of the easiest ways you can prevent unauthorized access to your funds and protect yourself is by using a hardware wallet to safeguard your assets.

If you continue using hot wallets, such as chrome extension wallets, please exercise strong security practices and know there is a risk of being compromised through software or social engineering tactics.

Guides To Using Ledger With Harmony

[Using Ledger with MetaMask](#)

[Using Ledger with Harmony Staking Dashboard](#)