

Forum:[Hack Forums](#)

Thread: [MetaMask?](#)

Thirty7 - November 16, 2025, 4:57 pm

I just started using MetaMask. Anyone have anything positive or negative to say about it ?[ph

Charlie Sheen - November 16, 2025, 5:01 pm

I loved MetaMask back when I was heavy into Ethereum projects.

Mewtwo - November 16, 2025, 6:19 pm

It's a hot wallet, I wouldn't recommend putting all your money into it.

Don't ever share your seeds to any website too.

DramaKing - November 16, 2025, 10:17 pm

Second the security concerns. There are public tools for cracking MetaMask vaults.

RangoWorld - November 17, 2025, 12:02 am

It was one of the first great self custody wallets. Still alright but now there are better options.

Hackers - November 17, 2025, 9:12 am

(Nov 17, 2025 01:02 AM)RangoWorld Wrote: [\[CITE\]](#) It was one of the first great self custody wallets. Still alright but now there are better options.

yeah agreed here, Metamask is one of the first to really thrive, so it'll be around for years based on that alone probably

I like MM but agree w/ other users here about security, hot wallet use, etc.

It definitely is good for Ethereum projects / web3 / etc.

Tyr - November 17, 2025, 10:26 am

(Nov 16, 2025 05:57 PM)Thirty7 Wrote: [\[CITE\]](#) I just started using MetaMask. Anyone have anything positive or negative to say about it ?[ph

<https://cloud.google.com/blog/topics/threat-intelligence/dprk-adopts-etherhiding>

All I gotta add for the time being apart from using it briefly 3 years ago only to realize it is a major security risk for certain individuals. Heard mixed things. Others can prob say more for you but I still urge you and anyone who uses MM to read this.

Hackers - November 17, 2025, 11:23 am

(Nov 17, 2025 11:26 AM)Tyr Wrote: [\[CITE\]](#)

<https://cloud.google.com/blog/topics/threat-intelligence/dprk-adopts-etherhiding>

All I gotta add for the time being apart from using it briefly 3 years ago only to realize it is a major security risk for certain individuals. Heard mixed things. Others can prob say more for you but I still urge you and anyone who uses MM to read this.Quote:Fetching the Malicious Payload: When a user visits the compromised website, the loader script executes in their browser. This script then communicates with the blockchain to retrieve the main malicious payload stored in a remote server. A key aspect of this step is the use of a read-only function call (such as `eth_call`), which does not

create a transaction on the blockchain. This ensures the retrieval of the malware is stealthy and avoids transaction fees (i.e. gas fees).

Payload Execution: Once fetched, the malicious payload is executed on the victim's computer. This can lead to various malicious activities, such as displaying fake login pages, installing information-stealing malware, or deploying ransomware.

Yeah... the amount of illegal content hosted on blockchain is staggering, and it's there "permanently". You can't remove malware or porn or anything from the blockchain without a hard fork, or without third-party software "fake ignoring it" while it's still there for all actual nodes