Solana Hack: How to Keep Your Crypto Wallet Safe?

Original: https://www.btcc.com/en-US/academy/research-analysis/solana-hack-how-to-keep-your-crypto-wallet-safe

One of the newest victims of crypto theft was a Solana blockchain-based cryptocurrency wallet. Some of the most popular hot Solana wallets have been hit by the hack. Mobile and web access to a hot wallet is possible. Tokens can be stored, sent, and received via this system.

There are many people who consider Solana a green token because of its use of the Proof-of-Stake mechanism. A single transaction on the network consumes less energy than two Google searches and 24 times less energy than charging your phone, according to the business. Here s a guide of how to keep your cryptocurrency wallets safe after the latest Solana hack.

1.Use a cold wallet to keep your cryptos safe

Storing your cryptocurrency in a cold wallet is the first line of defense against theft. One of the best ways to protect your cryptocurrency is to put your private keys (the crypto equivalent of your passcode) in a secure physical device. It is virtually impossible for hackers to steal your cash because it is virus-proof.

If your private key is compromised by a hacker who gains access to the server where your online wallet is stored, you could lose all of your hard-earned money in an instant.

2.Keep your crypto out of exchanges controlled by a single entit

'Nor your cryptos, not your keys' is the golden rule. Centralized exchanges have access to your private keys and can control your wallet, making them more vulnerable to hackers. It's critical to find out which exchanges have been hacked in the past so you can avoid placing your money at risk due to lax security methods or already-existing flaws.

3.Always keep your private key to yourself

There should never be any exchange of private keys. Keep in mind that anyone who obtains a copy of your private key has complete control over all of your digital assets. Private keys can be protected by

keeping them in a secure location and changing them frequently. Do not use the same private keys (passwords) across several sign-ins, such as Google or Facebook. Keep your private keys out of the reach of your computer and mobile devices at all times. Writing it down and keeping it in an area where only you have access to your keys is the best method to keep track of it.

4.Avoid connecting to public Wi-Fi networks

Never access your online crypto wallets or exchanges using public WiFi. Use a virtual private network (VPN) to mask your location and IP address if you don’t have any other options. A virtual private network (VPN) hides your real-world location and IP address, allowing you to conduct all of your online activities anonymously.

5.Watch out for phishing scams

One of the most prevalent methods used by cybercriminals to get your private keys is phishing. A free airdrop or giveaway will not appear when you click on a link in Discord, Twitter, etc. You should also be wary of any messages or chats that ask you to divulge your personal information.