# CNC Intelligence Provides Tips for Keeping Cryptocurrency Secure

WASHINGTON, DC, UNITED STATES, November 10, 2021 / EINPresswire.com/ -- The Justice Department recovered 2.3 million dollars in bitcoin paid to ransomware hackers by Colonial Pipeline in April.

According to the U.S law enforcement officers, they managed to recover about 2.3 million dollars in Bitcoin, a ransom that had been paid to cybercriminals by  Colonial Pipeline back in April.

It was not precisely known how the hacking was done. However, experts state that the FBI could recover the bitcoin ransom because of how the criminals stored their private keys. It dawned on them that the hack was not caused by any vulnerability within the cryptocurrency system.

The news made headlines and caused a significant stir online. Following the announcement, some speculated that the entire cryptocurrency was affected. This caused a decline in the bitcoin price. "Head of business development at bitcoin custody and loan firm, Park Lewis, said that anybody that has private keys can move funds at any time. He stated that securing private keys is very important since having them is the only way funds can be moved.

Nearly 82 million dollars was reported lost due to cryptocurrency scams. This occurred during the first quarters of 2020 and 2021, respectively. This figure represents ten times the amount lost during the same period the previous year. This is as reported by the FTC.

To ensure cryptocurrency's security from hackers and any potential threat, it's essential to understand the wallet alternatives available. This enables one to choose the best one to secure their private keys.

Below are some of the available alternatives to secure cryptocurrency compiled by the experts at CNC Intelligence;

· Adopt a Hybrid Outlook for Digital Wallets

Online wallets have gained popularity, therefore, attracting hackers' attention. The majority of consumers' cryptocurrency should thus be stored in offline or physical wallets. The remaining small amount can then be stored in an online wallet. This is according to Thycotis's chief information security officer, Terence Jackson. Thycotic is a Washington D.C.-based privileged access management solutions provider. He also reiterates that the physical wallet should be kept in a secure location like a safety deposit box to ensure its security.

· Having Two Strong Passwords is Key

Avoid reusing passwords at all costs, especially considering that cryptocurrency services have become key targets for hackers. Presume that all of them will eventually experience a data breach. This is according to Greenlights president Kevin Dunne. Greenlight is an integrated risk management solutions provider located in Flemington, New Jersey.

Despite cryptocurrency being an innovative technology that is progressing quickly, tested and practical security tactics are the easiest and quickest ways to secure a wallet, says Kevin Dunne. It would also help if one creates a solid and unique password for each to limit their exposure to the risk of hackers. Having a two-factor authentication and password which is rotation enabled would also be ideal. Employing a trusted password manager can help take the guesswork away by automating this process.

· Work with Reputable Cryptocurrency Wallets, Exchanges, Brokerages, and Mobile Apps.

Investors should carefully analyze each platform's security specifications to understand how their data will be protected before choosing which platform to use. Best security practices such as requiring multifactor authentication should be incorporated in a trusted security system. Air gapped devices that are kept offline and that have SSL or TLS encryptions would be the best to use, says Austin Merrets. Austin Merrets is an intelligence analyst at Digital Shadows, a digital risk protection solutions provider in San Francisco.

It can also be safer using more than one cryptocurrency platform, provided that owners use different and complex passwords for each forum. It is vital to maintain a secure password manager to safeguard their passwords, he says.

· Be Aware of How the Wallet is Used in Transactions.

According to the global vice president of New Net Technologies, Dirk Schrader, key "Cyber resilience" principles should be applied to cryptocurrency wallets. New net technologies is a cyber-security and compliance software company based in Naples, Florida. According to him, cryptocurrency is a good piece of data and code that holds a good amount of value for the

owner of the wallet and others.

The owner of the wallet should be conversant with how it is used in transactions. Ensure that networks and systems are not manipulated in case they are using them for transactions and have physical protection installed.

In a nutshell, it is crucial to acquire a sound security system to safeguard cryptocurrency from the risk of hackers. It is also essential to have a hybrid security system that has both physical or offline capabilities and offline capabilities. Having features like two passwords and double authentication can also be necessary for a formidable security system. Lastly, everyone should ensure that they work with renowned and trustworthy cryptocurrencies, brokerages, exchanges, and mobile apps.

Elliot Taylor
CNC Intelligence Inc.
+1 202-773-4704
email us here
Visit us on social media:
Facebook
LinkedIn