

Bitcoin Hackers run wild again: Cyber-Forensics.net explains how thieves steal funds-suggests bitcoin recovery measures

Officials from Cyber-Forensics.net highlight common scams targeting bitcoin users and suggest preventive ways.

SOFIA, BULGARIA, February 28, 2022

/EINPresswire.com/ -- Bitcoin scams are making rounds these days, tricking investors into spending in fake bitcoin schemes. The scammers are connecting with traders through social media apps, dating apps, text messages, emails and sending them messages with links to fake websites.

Once the site is opened, the potential targets are asked to purchase Bitcoin before communicating with the community of crypto space enthusiasts.

Cyber-Forensics.net, a cyber forensics service for online scam victims, threw light on the emerging cases surrounding bitcoin scams saying this type of online scam has tricked individuals in the U.S., South Africa, and the UK out of millions of dollars.

Chief analyst, Timothy Benson recalls: "The bitcoin scams I monitored turned out to reveal \$8.2 million stolen funds for an average amount of \$1.6 million per scam."

Further investigations by [bitcoin recovery companies](#) have found that scammers are leveraging compromised Youtube accounts, and other social media accounts to promote fake bitcoin schemes.

Here are some ways criminals steal cryptocurrency in the virtual world:

Hacking the Exchanges: Bitcoin and other cryptocurrencies are sold, bought, and stored on exchange platforms. But digital currency investors who organize the exchange object to centralized control which may lead to lapse in security. Thus, scammers may deploy malicious techniques to enter the user's server- simultaneously accessing passwords and enabling them to



Cyber-Forensics.net



Cyber Forensic Specialist



The bitcoin scams I monitored turned out to reveal \$8.2 million stolen funds for an average amount of \$1.6 million per scam."

Timothy Benson

move bitcoins from one address to another.

Hacking the Blockchain: Although quite rare and incredibly difficult-especially with major players like bitcoin, hacking a blockchain relies on decoding the interlocked blocks containing all transaction details. Since all blocks are interconnected, it is impossible to alter them. However, a theory claims that if a group obtains more than 50% of a specific blockchain, it is possible to rewrite transactions and block new ones.

Extortion: Many of cryptocurrency-related frauds have less to do with technology and more with old-fashioned tricks like extortion where criminals asked for direct transfer of digital currencies like bitcoin to release confidential information.

Best Practices to Avoid Bitcoin Scams:

Here are a few endeavors that crypto enthusiasts who want to avoid falling victims to bitcoin scams can take:

- Never take any information at face value. Make sure to investigate the matter individually being offered through anyone who claims to be a trader, investor, organization, or any successful business. Especially if the scheme sounds too good to be true or promises big returns overnight. It signals scam written all over it.
- Never trust anyone online: Whether they claim to be government officials, public figures, or strangers. They may be scammers who contact bitcoin investors asking for payments in cryptocurrency to double the amounts or offer "investment opportunity."
- Make sure to never share "private key" or the seed phrase to crypto wallet as it involves risks of third-party invasion.
- Enable two-factor authentication when using bitcoin wallets and any exchange medium.
- Double-check website URLs as they might be fake websites attempting phishing scams. Ensure to look for letter swaps and numbers like- "l" for "1" or "O" letter for the number "0",
- Reject any offer that asks for up-front fees-especially if it comes from an unknown source.
- Look for red flags that indicate a bitcoin scam on its way. For example, 1) promising unrealistic returns in a short period 2) if a scheme promises bitcoin giveaways and asks investors to send a few coins for address verification.

Best way to ensure not losing any bitcoin funds is to do diligent research. It can be a bit of a task but will ensure not falling into the fake crypto ecosystem.

How to Report Bitcoin Scams?

1) Contact Local authorities: If anyone encounters such a type of bitcoin scam or thinks they

have been victims of scams, contact the local authorities as soon as possible. Also, report the matter to nearby Trade commissions and Security Exchange Commissions.

2) Report Exchange platforms: It's also a good idea to report the bitcoin scams to exchange platforms through which transfers were made.

How to Recover Funds from Lost Bitcoin Wallets?

Many owners of the most powerful cryptocurrency i.e bitcoin have lost access to their account. Reports mention a staggering loss of \$100 billion- but some is recoverable.

Cyber-Forensics.net, a [bitcoin fund recovery company](#), estimated that traders who have lost access to digital currencies may increase chances at bitcoin fund recovery with the help of high-tech firms.

[Forensics Recovery](#) expert Peter Thompson says "Of course, not all digital assets are recoverable, but there is always a decent chance of getting the loot back if victims had encrypted private keys to bitcoin wallets but forgot password or if they had a failed hard drive with private keys."

About Cyber-Forensics.net

Cyber-Forensics.net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. Cyber-Forensics.net commonly deals with Bitcoin scams and Forex withdrawal problems. For more information, please visit <https://cyber-forensics.net/>.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613
[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/563156293>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 IPD Group, Inc. All Right Reserved.