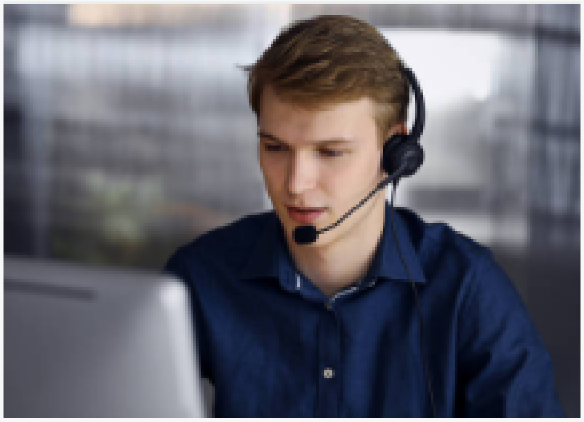
EINPRESSWIRE

Cyber-Forensics.net’s comprehensive guide to ICO: Timothy Benson explains everything businesses should know about them

ICO has yielded massive success as a popular method to raise money to create new digital coins. But the platform is also attracting scammers.



Cyber Forensic Specialist

Cyber-Forensics.net

SOFIA, BULGARIA, April 18, 2022 /EINPresswire.com/ -- Initial Coin Offerings (ICOs) has opened new avenues for investors in blockchain ventures. As per reports by leading websites, in the third quarter of 2017 alone, ICOs raised more than $1.3 billion for cryptocurrency companies. The figure is five times higher than funds raised through capital ventures.

Cyber-Forensics.net, a cyber forensics service for online scam victims, says, “with exponential growth in ICO by the public, it is no surprise that ICOs have been used to fund scams and trick investors.”

Adding to the statement, crypto theft investigator Timothy Benson explains, “not every project is fake or fraud, but all the hype around ICO is worth investigating the platform for potential disruption. There are several variants of ICO scams prevalent online. Therefore, a comprehensive, detailed study can be instrumental when the goal is consumer protection.”

> “
> with exponential growth in ICO by the public, it is no surprise that ICOs have been used to fund scams and trick investors.”
>
> *Timothy Benson*

Types of ICO Scams:

 Exit Scam is a fraudulent operation organized by unscrupulous crypto promoters who collect investor funds for an ICO and disappear. 2018 witnessed more than $100 million lost in ICO exit scams.
 Bounty Scam: Another common ICO scam, Bounty scam fails to pay out promoters' promised financial rewards for PR activities.

- Exchange Scam: Developers mislead investors to put money in a fake exchange.
- White Paper Plagiarism Scam: Scammers copy the white paper of genuine ICO firms and decide to launch similar projects under a different name.
- URL Scam: Criminals build fake websites that match ICOs and instruct users to deposit digital coins into a corrupted wallet.

How to identify ICO Scam?

There are several ways to identify ICO scams and sketchy scammers:

- Read the whitepaper: To avoid ICO scams, read projected whitepapers related to a scheme and gain deep insight. Whitepaper usually lays out business strategies, goals, background, concerns, financial models, SWOT analysis, and the estimated project completion timeline. Investors must avoid associating with companies that don't issue whitepapers.
- Understand the team: It is recommended to do thorough research on individual team members of the said project. Users must understand the administrative units by checking their business profiles. Go through social media platforms to match credentials before investing in the project.
- Evaluate intensity of promises: Whitepapers are an excellent source for analyzing business intent. Anything that seems out of place must be reported. Moreover, check the company's profile on platforms like Google, Crunchbase, or Comparably.

What to do if you are scammed in an ICO Scam?

Cybercriminals are very convincing. They can reach their potential targets through email, text, SMS, social media apps in hopes of stealing personal information and, ultimately, money.

And they are extremely good at what they do. However, there are a few things to pay attention to if someone is scammed into an ICO fraud.

There are two ways someone could have been targeted: a) individuals either sent crypto-coins to scammers or b) shared personal information.

When sent money to scammers:

- Contact the bank and request them to cease all unauthorized transactions. Tell them about the fraudulent activity. Ask for reversal of transactions.
- Get to know about unauthorized debit or withdrawal.
- Contact local police or nearby law enforcement agencies.
- Connect with a wire transfer company (if money was sent through wire transfers).
- Report the fraudulent transfer to the company behind the money transfer app (if the money was paid using a money transfer app)

When someone shared personal information with scammers:

- Keep monitoring credit card activity.
- Plus off computer/ device from the internet.
- Create a new password for the apps on phones.
- If possible, reset computer software and install new updates.

How to Report an ICO Scam?

Reporting lost cryptocurrency or ICO losses apply different methods in different situations. For example, in the United States, the most common crypto scams are usually listed on popular crypto scam lists online. Each fraud in the state will fall within three categories: 1) Casualty loss, 2) Theft loss, and 3) Investment loss.

The first and foremost step is to report the matter to local police or law enforcement agencies in each case. When someone is deprived of their money with a criminal intent to cause financial damage, reporting the matter is the only approach to qualify for necessary help.

Timothy Benson, the crypto-asset recovery specialist at Cyber-Forensics.net, says, “the correct way would be to treat lost cryptocurrency and ICO scam as a capital investment loss and obtain a report from local police, SEC, or financial crime investigators. The information will be used in IRS audit protection.

How to Get Money from an ICO Scammer?

Gather Proof: Collect as much information as possible before making any move. Get to know how the company corresponded. Track their advertisements, etc. Any screenshot is helpful in the eyes of the court. Stack up the necessary evidence against fraud ICO companies or individuals. Another thing to do is keep the list of evidence and their whitepaper as a roadmap. The purpose is to project how the company hasn’t fulfilled its promises.

File a case: The next step is to file the case as per the rules and regulations of the country. The tricky part is to figure out who to hold responsible. For this, take help from the best crypto recovery services. The team will analyze the market and do quick research on how to convict ICO fraudsters.

If victims of ICO fraud want to find out about good crypto recovery services, read online reviews and do a background check. Based on multiple site reviews, Cyber-Forensics.net is a recommended name in the field.

About Cyber-Forensics.net

Cyber-Forensics.net is the world’s leading fund recovery company that offers fund tracing and recovery services to the victims of online scams including romance scams. It works around the clock to assist consumers and corporate clients across the world who are facing or at the risk of facing online financial scams. For more information, please visit https://cyber-forensics.net.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613
email us here
Visit us on social media:
Twitter