

# Cyber-Forensics.net says crypto scammers fake it till they make it: Here is how investors can protect their coins

*Fraudsters may use variants of crypto scams to reach targets and steal digital tokens/funds. Cyber expert Timothy Benson lays out ways to protect crypto coins.*

SOFIA, BULGARIA, March 22, 2022 /EINPresswire.com/

-- Cryptocurrency crimes have shown a record-breaking increase in the past few years. A blockchain analysis firm released a statement informing "digital currency scammers took \$14 billion worth of coins in 2021. This figure is nearly twice the amount that scammers looted in 2020."

Chief analyst Timothy Benson at Cyber-Forensics.net, a cyber forensics service for online scam victims comments, "With the boom in cryptocurrency, it's no wonder that cybercriminals have taken notice of opportunities for conducting illicit activities." Crypto will continue to attract online scammers despite the high-tech nature and complexities.

Based on complaints received by Cyber-Forensics.net, the firm notes that there are approximately 7,000 people in the United States who lost over \$80 million worth of crypto from October 2020 through March 2021. In addition, scammers use multiple and highly sophisticated new tactics to trick people.

Benson stated further, "scammers may give a new face to their gimmicks every time they find a new target, but in one way or another, they follow some pattern that investors and traders can look out for."

## Types of Crypto Scams

□ **Demanding Crypto-Only Payments:** This type of online scam seemingly involves scammers posing as official firms claiming that they cannot accept payment in any other form than cryptocurrency. In general, when anyone pressurizes traders/investors to pay in popular coin forms like Bitcoin, it is likely a scam.



Cyber-Forensics.net



Cyber Forensic Specialist



Fraudsters may use variants of crypto scams to reach their targets and steal digital tokens/funds. Cyber expert Timothy Benson lays out ways to protect crypto coins.”

*Timothy Benson*

Moreover, blockchain technology doesn't require a physical presence to open an eWallet. Thus, it's easy for scammers to open wallets without verification or contact information.

□ Digital Collectibles Crypto Scams: Crypto scammers can create new games using sophisticated codes and create an entirely imaginary blockchain world. As they do it, this provides an easy way for crypto hackers to generate excitement around their fake games and lure young

entrepreneurs into transferring their crypto coins to buy a newly minted game or coin.

□ Crypto Investment Scams: Of course, the most obvious way to steal crypto coins from investors is by luring them into spending their funds on prolific investment schemes. But Cyber-Forensics.net warns that these investment schemes can be a fraud. Crypto scammers set up fake social media accounts, fake IDs, websites to sound legit and claim to offer a once-in-a-lifetime opportunity.

Cyber thugs now that the investment sector is ripe with traders who are willing to take risks on investments that can bring positive returns in the future.

□ Using Fake Identities to Steal Crypto: As already mentioned, setting up a digital wallet doesn't require the individual to be physically present, which allows scammers to build fake profiles by providing wrong information. “The lack of KYC protocols on the blockchain is a major question mark for its widespread use,” commented Jonathan Padilla, former PayPal head.

Adding to the statement, [Crypto recovery](#) expert Peter Thompson says, “since there are no safeguards in decentralized platforms, crypto scammers can fake it till they find their target.”

On a good day, they might even steal a huge amount of crypto coins from investors, which is why it becomes highly crucial to protect them.

### How to Protect Cryptocoins?

Even the most technologically advanced cyber security firms acknowledge that cryptocurrency is full of risks. And these risks are ever-evolving. Even though the world is leaping towards online structures that claim to be completely safe, all platforms are prone to cyber attacks.

Never invest entire crypto funds in the blockchain: Nobody is immune to crypto scams- an experience that blockchain investor and entrepreneur Ian Ballina who lost \$2.5 million, would never forget. Ballina ended up losing millions of worth of crypto coins after his information was

compromised by someone who hacked into his account.

Ballina's story highlights that losing crypto coins isn't that difficult, but recovering them can be. Further, mining scam experts explain that when dealing with such volatile assets, it is advised to keep crypto holdings to under 5% of their total investment capacity.

Know the Crypto Red Flags: Watch out for the standard warning signs similar to other scams like credit card fraud:

Typographical errors and obvious spelling mistakes in text messages, emails, and social media.

- Anything that promises to multiply money in a shorter duration.
- Contractual obligations on payment mode.
- Risk of potentially locking crypto coins.
- Fake social media influencers claiming to be celebrities.
- Beware of psychological manipulation tricks like extortion or blackmail.
- Schemes promising free money.
- Vague details about an investment scheme.

Know when to contact higher authorities: The best way to protect crypto coins is by contacting the [best crypto recovery service](#) providers.

In addition, when someone believes that they are about to be trapped into a crypto scam, they should immediately contact the local authorities of their area and, if possible, also hire crypto recovery services.

A professional team of cryptocurrency scam solutions firms will adopt best-in-class strategies to know how scammers targeted their victims and stole digital coins.

How to Report a Stolen Cryptocurrency?

When someone believes crypto scammers have targeted them, they should immediately report the suspicious activity involving crypto to the following authorities:

- The Federal Trade Commission (If the victim is a resident of the United States) at the following website: [ReportFraud.ftc.gov](http://ReportFraud.ftc.gov)
- The Commodity Futures Trading Commission (CFTC) at [CFTC.gov/complaint](http://CFTC.gov/complaint)
- The U.S. Securities and Exchange Commission (SEC) at [sec.gov/tcrlf](http://sec.gov/tcrlf) if the fraud involves extortion or blackmail.
- The victims can also take help from fund recovery experts to [recover stolen crypto](#).

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](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/565698488>

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.