

From fake websites to apps, Crypto scammers are everywhere: Cyber-Forensics.net promotes safety first culture

Cryptocurrency has caught the attention of marketers looking to make money quick and scammers have taken note too. Here are tips to stay protected.

SOFIA, BULGARIA, March 24, 2022 /EINPresswire.com/ -- Cryptocurrency scams have jumped up in numbers. They are 66% more dangerous than any other online scam causing financial losses. U.S. authorities are on alert mode after Michigan state police tracked 31 scams related to crypto currencies.

Investigations led by the state department identified several websites and applications created by scammers to beguile innocent victims.

Another cyber security firm, Cyber-Forensics.net, a cyber forensics service for online scam victims says, bitcoin scams involve deceiving targets or potential targets into paying funds either in the form of coins/tokens or invest their available funds into fraud investment schemes.

But individuals can stay protected if they know when they can be targeted potentially and what it leads to:

Types of Bitcoin Scams Running Online:

A) Investment and Business Opportunity Scams: Illegal organizations promise investors large returns on small investments in a short time and achieve financial freedom.

Such scammers may also pose as knowledgeable crypto enthusiasts looking for an opportunity to grow their business. But in reality, they only want to grow their profits. Scammers will say participants can win reward points meaning more cryptocurrency if they pay.

Some scammers conduct their tricks by sending unsolicited offers from fake profiles. They may also pose as investment managers. But once the victims put money into the suggested account,



Cyber Forensic Specialist



Cyber-Forensics.net



Such scammers may also pose as knowledgeable crypto enthusiasts looking for an opportunity to grow their business. But in reality, they only want to grow their profits.”

Timothy Benson

victims will realize that they can withdraw their profits only if they pay some amount of bitcoins.

Another popular way is where scammers may send a list of fake employment offers on websites. They will promise a good job but end up taking the victims' money or stealing personal information.

B) The Classic Blackmailing Emails: Fraudsters will often send emails to recipients containing a link to victims' personal photos, or videos. Scammers use this data to

blackmail crypto holders into paying the desired funds. In usual cases, victims do what is asked of them out of fear.

But [bitcoin recovery](#) specialist Timothy Benson says: “Don’t do it. This comes under criminal extortion. When someone faces such a problem, report it to the local authorities immediately.”

C) Social Media Bitcoin Scams: Interestingly, modern day scammers have realized that social media is a ripe field to find targets without much effort. Platforms like Facebook, Instagram, Twitter, WhatsApp attract quick responses from online users. Additionally, scammers can find a huge number of audiences in one go. This is also the reason even the best [bitcoin scam recovery](#) services are observing an increased number of cases. Some scammers may open fake celebrity accounts identical to genuine accounts to encourage fans to put bitcoins into fake accounts.

Why is Bitcoin Recovery so Challenging?

Despite the claims that cryptocurrency is fundamentally a safe platform, there are always scammers who identify ways to break the ecosystem- especially where online infrastructures are not based on blockchain. These principles can be violated by scammers. Additionally, many blockchain protocols are decentralized which risk the integrity of the capital in the wallets.

How to Avoid Bitcoin Recovery Scams?

Scammers are always looking for ways to steal money from unsuspecting victims. In fact, tricksters may even stoop as low as targeting the scam victims again in the name of pretending to help the victims.

One sure sign to avoid an upcoming bitcoin recovery scam is by practicing security first culture online. For example,

- Safeguarding private keys to bitcoin wallets.
- Not sharing private keys to anyone online.

- Identifying the threats to computer networks.
- Learning about safety measures for bitcoin storage
- Implementing multi-factor authentication to access wallet
- Checking site URLs before clicking them

Gathering information: Do a thorough research before investing into any project. Don't take anyone's word on face value.

How to Report the Bitcoin Scam?

Report suspicious activities involving bitcoins to either of the law enforcement:

- Local authorities of nearby area
- Trade commissions
- Securities and Exchange Commission

Regardless of the method of bitcoin scam used to target victims, victims may suffer financial losses. Therefore, raising the matter by reporting it should be one of the steps in order to stay protected in future.

In addition, contacting appropriate agencies can leverage victims' chance to recoup lost funds. Fortunately, bitcoin funds can be tracked, although the task is challenging.

Fund recovery companies like Cyber forensic have an extensive experience to identify the perpetrators behind the scam and help victims build a strong case against tricksters.

How do Bitcoin Recovery Services Secure Victims' Funds?

[Bitcoin recovery service](#) suggests crypto recovery is a multi-layered process. But some of the key points of it are as follows:

- Investigating third-party security risks: To illustrate the critical importance of security risks, bitcoin recovery services obtain complete information behind how the scam happened including if victims downloaded fraudulent third-party apps.
- Mistaken transactions: Since bitcoin transactions are irreversible, experts recommend being careful when sending/receiving bitcoins. But if victims happen to transfer their digital assets to someone by mistake, the only way to recover bitcoin sent to incorrect addresses is to trace the owner of the address.

What to do if scammed into Bitcoin Scams?

When someone believes they have been scammed into sending their finances to someone

online, the first and foremost protocol is to bring the matter to the notice of local authorities. An explanation of how the online scam took place and how the perpetrators got to their potential targets can prove beneficial to investigators in retracing how the scam occurred. Also, it saves emotional distress for victims to relive the experience every time they are asked to explain what happened.

As the world faces a growing number of bitcoin scams, the best thing to get money back is to talk to fund recovery services. Firms like Cyber-Forensics.net are equipped with tools and equipment to ease the fund recovery process.

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/566051611>

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.