

FBI Warns About Recovery Scams

The [FBI is warning organizations](#) of an increase in scammers pretending to be recovery companies. Cyber recovery scams, also known as data recovery scams, play on the vulnerabilities and emotions of individuals who have experienced data loss or other digital disasters. These scams typically target those who are desperate to regain access to their important files, documents, or accounts that have been compromised due to malware, ransomware, or other cyber incidents. These scammers are advertising their services in the comments section of well-known websites that cover technology news. Additionally, fake recommendations on these comments makes the advertisement appear like a legitimate service that is endorsed by the website.

2808 comments

TO RESTORE LOST BITCOIN;CONTACT CAPTAINWEB GENESIS.

After a long research on Crypto Recovery, I came across a Bitcoin expert who recommended me to a Legitimate Recovery Expert CaptainWeb Genesis, a specialized hacker with Cyber skills to help Scam victims recover Lost Crypto. I was curious at first about my trust to work with the Expert, luckily enough all my funds were able to be recovered and transferred back to me within an hour by CaptainWeb Genesis.

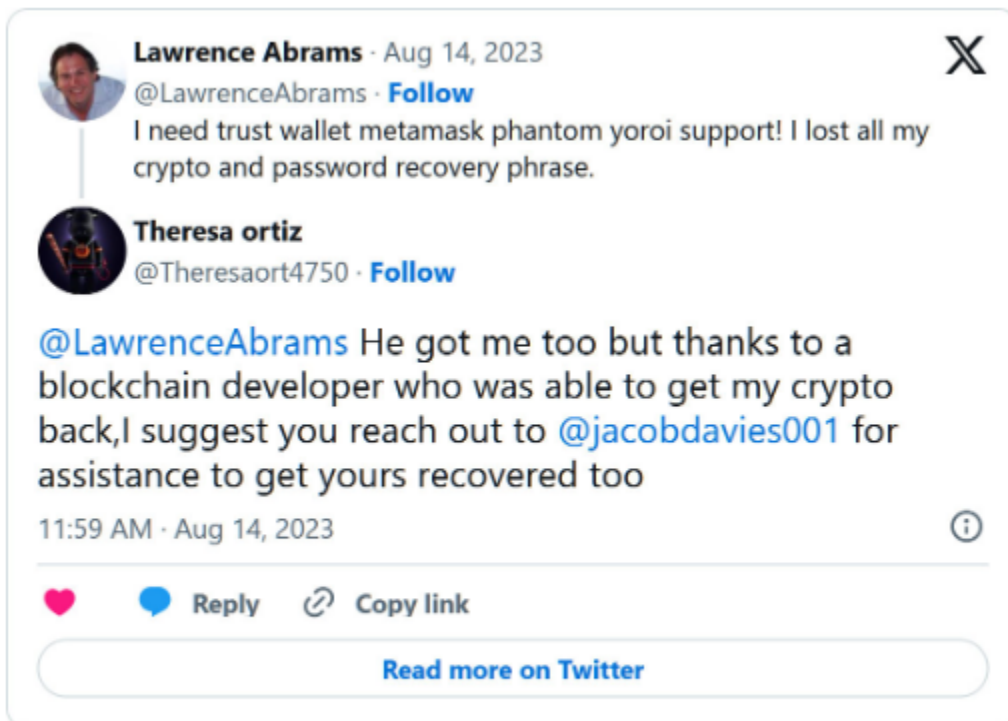
Simply file a complaint through the CaptainWeb Genesis Website and find your lost Btc/Crypto transactions back through the Experts services.

Contact info Web ht://.....
Mail C:.....

Don't forget to mention that Hannah Vilde recommended you.

— Hannah Vilde August 01, 2023

Comment promoting fake crypto recovery services (*BleepingComputer*)



The screenshot shows a Twitter thread. The top tweet is from Lawrence Abrams (@LawrenceAbrams) dated Aug 14, 2023. The text of the tweet reads: "I need trust wallet metamask phantom yoroi support! I lost all my crypto and password recovery phrase." Below this is a reply from Theresa ortiz (@Theresaort4750) dated Aug 14, 2023 at 11:59 AM. Her reply says: "@LawrenceAbrams He got me too but thanks to a blockchain developer who was able to get my crypto back, I suggest you reach out to @jacobdavies001 for assistance to get yours recovered too". The interface includes a heart icon, a reply icon, and a copy link icon. At the bottom of the thread is a button that says "Read more on Twitter".

Twitter bot pushing cryptocurrency recovery scam

Source: BleepingComputer

Once the scammer receives payment, they either cut off communication with the victim or will attempt to solicit additional

funds. These additional funds are claimed to be due to more resources needed to complete the recovery of funds or information. This can lead companies to pay exorbitant fees for the supposed recovery services.

Protecting Your Organization from Cyber Recovery Scams

Exercise Caution: Be wary of unsolicited communications offering recovery services, especially if they claim to have found your information without your prior request.

Verify Credentials: If considering a recovery service, research the provider thoroughly. Verify their credentials, reviews, and legitimacy before making any commitments.

Backup Regularly: The best defense against data loss is to have regular backups. This minimizes the impact of ransomware or other incidents, reducing the pressure to pay scammers.

Beware of Payment Requests: Never make payments to individuals or organizations you're unfamiliar with, especially if they demand immediate payment using cryptocurrencies or other untraceable methods.

Contact Trusted Experts: If you're in need of data recovery, consult reputable professionals or organizations that you trust or that have been recommended by trusted sources.

Educate Yourself: Stay informed about the latest cybersecurity threats and scams. Regularly educate yourself and your team to recognize and avoid potential risks.

Cyber recovery scams are a distressing consequence of the evolving cyber threat landscape. By staying vigilant, researching recovery services, and following best practices for cybersecurity, companies can protect their organization from falling victim to these malicious schemes. Remember that legitimate recovery experts prioritize companies interests and will never pressure the organization into making a hasty decision. With the right precautions and awareness, your organization can navigate the digital world with confidence and security.

The CRITICALSTART® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. The CTI team will post any future updates via Cyber Operations Risk & Response™ Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://www.bleepingcomputer.com/news/security/fbi-warns-of-increasing-cryptocurrency-recovery-scams/?&web_view=true