# Tether-Hack Victim Watches Cryptocurrency Vanish from Account, Only to Encounter Frustrating Customer Service

CHIAYI CITY, TAIWAN, September 12, 2021 /EINPresswire.com/ -- Tether-Hack Victim Watches Cryptocurrency Vanish from Account, Only to Encounter Frustrating Customer Service

Cryptocurrency theft is one of the fastest-growing cyber-crimes in the world today. As more and more people have taken an interest in cryptocurrency, there has been an ever-increasing number of complaints that have revealed a pattern of account hacks in which users have reported money vanishing from their accounts. Worse yet, when victims of these hacks try to contact cryptocurrency platforms for support, they often encounter an even more frustrating experience. This is exactly what happened to Liu Kun-Hung, an antique dealer in Taiwan.

According to local police in Taiwan, Liu's US$3.1 million worth of digital currency was stored in two Tether accounts in the United States. In early July, Liu noticed three unknown transfers from the accounts and immediately knew that they had been hacked. Liu quickly changed the account passwords several times, but even this failed to stop the unauthorized transfers. He then contacted the service department at Tether. After doing so, he was asked to call the local police and report the stolen funds, if he had plans on taking legal recourse in an attempt to get the money back. After Taiwan's Criminal Investigation Bureau got involved, Tether was able to freeze the remaining US$2.6 million that had been diverted to the unknown cloud wallets, the police said.

Liu has stated that when a customer discovers that his or her cloud wallet has been hacked and money has been drained from it, this should definitely be considered an emergency. Unfortunately, the customer service he has received has been conducted primarily via email, and it has often been difficult to reach representatives. To make matters worse, in many cases, these types of losses might become permanent because all transactions are pseudonymous and typically irreversible. Liu believes that these companies should do better, or at the very least, they should treat these situations as an emergency, responding to and helping out customers as quickly and effectively as possible, and not making the victims of hacks feel helpless or angry.

Despite being baffled and frustrated, Liu hopes other people will be able to learn from his experience, and he has again urged these companies and platforms to improve their policies and protocols. In the meantime, those who suspect their cloud wallets have been compromised are encouraged to act as fast as possible to safeguard their funds.

The following are a few tips from Liu's experience, for when a worst-case scenario occurs:

If you notice any transactions going out of your digital wallet that you didn't make, you have probably been hacked and your funds can be drained within minutes.

To start, try to create a new digital wallet as fast as possible and transfer all the funds there, if the attacker does not already have access to them. At the same time, quickly change the log-in details of the account and be sure to activate two-factor authentication to lock out the attacker.

Contact the police. The police will log the crime and create a crime reference number. Also, reporting this to the police will help if you plan on taking any legal recourse to attempt to reclaim the stolen funds.

It is highly advisable to check all of your electronic devices for any malware. Crypto-stealing malware is a popular tool used by cybercriminals to carry out a cloud-wallet hack. So, it is only wise to scan all of the devices that are used to access your cloud wallet and ensure that they are completely free of any hostile software.

Despite all of these frustrations, people should still notify the cryptocurrency company, and let them know about the breach and the fraudulent transactions. By doing so, crucial information about the illegal transactions may be obtained, and this could be useful in the investigation.

Liu's case is still under investigation. Based on the information obtained in the initial probe, it appeared that the hackers stole the password and vital account information by hacking into his cell phone. According to Taiwan's Criminal Investigation Bureau, investigators have already identified the hacker's internet protocol address, and this address is linked to a cloud-service provider in New Taipei City, Taiwan.

George Hu
Verdancy Company
+886919563599 ext.
email us here