February 21, 2022

OVATION
AMERICAS

March 2022 Newsletter

CRYPTO WALLET PRIVACY & SECURITY (Part 1)

Crypto scam revenue in 2021 topped $7.7 billion, up 81 percent compared to 2020, according to the blockchain data platform Chainalysis.

Your crypto wallet privacy and security is a crucial part of how much you will be successful investing in crypto. Once you hold your cryptocurrency in wallets, you need to be aware that all types of crypto wallets – even the most secure hard drive wallets – are exposed to some risk of being hacked and drained. While blockchain technology is designed to be extremely secure, and a blockchain database is nearly impossible to hack, human error and physical risks still exist. The risks may vary and constantly change, but here are some of the most widely-seen ways to lose all your cryptos overnight.

Key-Stealing Malware

A key-stealing malware scans the hard drive of your computer or mobile device for your crypto private keys. A key-stealing malware can enter your device when you visit dubious websites, follow links from scammers, open unsecure email attachments, or download software from untrustworthy sources. Once you download a key-stealing malware on your computer or a mobile device, it instantly scans the hard drives for your crypto private keys and transmits them to a hacker. If you do not secure your crypto wallets with two-factor authentication in addition to the key, the person controlling the malware will now have the access to your accounts and be able to transfer your holdings in a matter of seconds.

Trojan

A trojan is another type of crypto-stealing malware. Trojans do not actually “steal” your cryptocurrencies but scan your hard drives for the exact amount of cryptos you own. Then they maliciously encrypt your hard drives and send you emails and display messages to demand ransoms. Even well-protected exchanges might encounter such ransomware, and sometimes users have no other way to deal with the dilemma when the ransomware threatens to format the hard drives if the users do not pay the ransom within a certain period of time.

Exit Scam

An exit scam refers to when exchanges, intermediaries, or managers disappear with investors' money. It is a crypto spin on an old confidence trick that has been around for centuries. In the past, fund managers or startup founders may run off with investors' money. In the crypto industry, exchanges may vanish with their users' deposits; managers or owners of crypto projects could run off with the funds collected from an initial coin offering (ICO). Due to the decentralized and anonymous nature of the crypto world and limited regulatory frameworks, it can be more difficult to trace the scammers and recover the funds compared with traditional scams. Exit scams take place frequently, Users need to learn how to spot potential scams before they make any crypto investments.

Phishing

A phishing attack is usually conducted via emails, messaging, or social media. You might receive an email or a message that asks you to take actions including sending your authentication code, password, credit card number, or other credentials. However, the email is not legitimate, or attempting to impersonate someone else. If you reply to those phishing emails and give them any information, your crypto holdings can be stolen. Do not trust anyone who asks for your credentials and passwords.

Device Loss

After all there is the old-fashioned way to lose your belongings – to literally lose your mobile devices (or laptops). Anyone who finds your device or physically steals it can proceed to attempt to unlock it as well. If they succeed in unlocking your device, they can gain access to your crypto holdings stored in the wallets on that device, as well as your banks accounts, emails, passwords, social media accounts, and anything of value connected to your device.

How to Protect and Secure Your Holdings

1. Take basic Internet security measures. Use strong, updated passwords. Don't visit suspicious sites or click on suspicious links. Don't use "free WiFi". Use Internet security tools like antivirus programs and VPNs. Activate 2-factor authentication for all your accounts.

2. Remember that you are the weakest link. Actually hacking the code of a blockchain or getting through the security system of a website is very difficult and requires specialized skills that most criminals do not possess. It is far easier for a thief to impersonate a trusted party or send you compromised links in the hope that you will click on them.

3. Always be cautious and double-check every notification you receive. Caution keeps you away from dubious crypto promoters, suspicious exchanges that may vanish anytime, phishing emails and messages, etc. Choose your software and application downloading sources wisely – official websites and stores like Apple's App Store can be a good choice (although the Google Play Store has been identified as a major source of Android malware). If a reminder pops up when you try to access or download anything, read the reminder and have a

second thought about whether you still want to access and download whatever you planned to.

4. Given all the risks and scams mentioned above, It is preferable to control your own locally-stored wallet with an open-source software application which stores, accepts, and transmits virtual currencies directly from your computer, one of the safest option for securing your cryptocurrency assets. When your wallet is disconnected from the Internet, no hacker can directly see and attack it.

   It is estimated that 23% of all cryptocurrencies have been lost due to inaccessible wallets, if you delete the file or lose access, you have lost your money inside. Please do not be part of this statistic. We consider virtual currencies as a tool among others to protect privacy or anonymity online and never an investment. Overall, most of our clients have no use for it.

Crypto security is very much a matter of good personal habits. Let's keep learning and stay up to date on cybersecurity issues to give us the best chance of avoiding costly hacks and scams.

OVATION
AMERICAS