Epoch Sec

STAYING SAFE IN CRYPTO

TABLE OF CONTENTS

OVERVIEW

The overall premise of this document is to give the average user some guidance on better protecting yourself, specific to interactions with Crypto / Blockchain activity.

This document is facilitated and guided by one of Latheesan's posts. I had this topic in mind, but when I saw he covered this, I wanted to use his content and messaging. (Yes, I had approval).

FUNDS ON EXCHANGES

Take your funds off of exchanges

- Leaving your funds on exchanges is a risky habit. Exchanges can:
    - Lock your funds and halt withdrawals without any notice. This may change when regulation inevitably comes into the picture.
    - Misuse customer funds. For example, reinvest customer funds, held by the exchange, for other investments. I will not get into the legal repercussions, but keep in mind this is not an allowed behavior.
    - Go insolvent. Meaning "unable to pay debt". This also means that they may not have the funds to deliver to customers when they want to withdrawal
    - They are also susceptible to being compromised (attacks, hacks, etc)
- You may be able to get a higher APY on exchanges, but typically this is not sustainable. And is it worth the risk?
    - I prefer to keep the mindsight as: "I would rather miss 9 out of 10 opportunities, instead of getting compromised 1 out 100 times."
- Stake your Crypto with Community Stake Pools. Do not rely on an exchange having custody of your funds. This means that they technically have full control.
- Only use an exchange for it's intended purpose. For exchanging crypto <> fiat. Do your business and get out.
- Remember the most recent exchange stories: Voyager, Celsius, FTX

HARDWARE WALLETS

Invest in hardware wallets

- Keep your funds safe in cold storage.
    - Two great popular options are the Ledger and the Trezor (Model T is my preference).
        - Buy these hardware wallets directly from their source. Do not buy from third parties. You cannot be sure they are safe to use, otherwise.
    - It's easy to think "that is so much hassle". But there more you do/use it, the more routine and natural it becomes. The hassle is worth it.

ENABLE SIM LOCK

Sim Lock your phone SIM

- Sim locking
    - Feature that is most commonly overlooked.
    - Requires authentication for accessing a SIM.
- An attack becoming more common is that a bad actor will attempt to socially engineer your service provider and convince them into sending the bad actor, a replacement SIM. This will in turn allow them to receive your calls, SMS, and any OTP / 2FA SMS authentication messages.
- Android, for example, has the SIM locking feature in “settings”. You can enable this and set a pin for authentication to unlock the SIM.

WALLET SEED PHRASES

Store your wallet seed phrases securely

- Try not to confuse the purpose of seed phrases and passwords
    - Seed Phrase is used to allow you access to the wallet. If another persons gains your seed phrase, then they have full access to your wallet
    - Password are typically use in a wallet for signing transactions. I can restore a wallet to another device, then create a new signing password, if I had the seed phrase.
- Use a metallic storage device for your seed phrase. Keep that in a safe.
- Do not leave your seed phrases or password on your desktop, laptop, or mobile device! If you are compromised, if someone gains access to your system, if you get a keylogger unknowingly. All of these can allow the bad actor to get your seed phrase if you store it digitally.
    - CK_Wallet or Crypt Keeper wallet is a great option.

PASSWORD MANAGER

Password managers can help manage complicated password when you have many accounts.

- It is common for individuals and teams to use the same account and password for many accounts they have. Another habit to use the same username, but slightly change the password each time a new account is made on a new application, or website, etc. The problem is if a bad actors gains your password, they can then log into any other accounts you may have. Or they can easily brute force additional passwords.
- Use a password manager. Create different, complicated password for every account. We all have many accounts for multiple email accounts, websites, cryto sites, retails site, and so on. But you can use a password manager to maintain your encrypted passwords. Then create another unique password for the password manager. That is then what you routinely use.

    - Examples: Lastpass or Keypass, bitwarden, 1password, and Dashlane
- Be careful with using password managers, as you would with any other application. For example, Lastpass released that they had user data compromised. I believe that Bitwarden (and possibly 1password) has self hosting.

USING 2FA

- Two Factor Authentication software and hardware device require a second authentication, once you authenticate with your password to different applications.
- Google Authenticator is an example of a software 2FA application
- Yubikey is an example of a hardware 2FA device. This is arguably more secure. However, using either one is better than not using 2FA.
- Suggestion: Do not use SMS two factor authentication when possible to avoid.
- With 2FA + Sim Lock, you are greatly decreasing your odds of being attacked or compromised.

CONCLUSION

DO NOT BE AFRAID TO MISS AN OPPORTUNITY!

If you are not confident in a project or tool, do not engage and participate until you are confident. I would rather miss 9 out of 10 opportunities, instead of getting compromised 1 out of 100 times. It only takes once.

Keep in mind an easy tactic used by bad actors. That is obfuscation and is used along with Social Engineering and Phishing, which are the two most common attack methods (using vehicles such email, websites, and social media). Obfuscating is taking a domain URL, discord user or server, Twitter Account, or Telegram Account and make a very slight change in hopes that the user/target does not notice. So pay attention!