BLOCKWARE SOLUTIONS

February 23, 2020

How to Properly Secure Your Digital Currency - a Step by Step Guide by Blockware Solutions

Abstract:
There is inherent risk for users holding digital currency on an exchange. Hackers target exchange users because the hacker knows that there will likely be digital currency readily accessible. Unsecure smartphones and email accounts are the two primary points of failure that hackers frequently exploit. Most exchanges require 2 Factor Authentication (2FA) to secure user accounts but relying on a phone number (SMS - text messages) for 2FA is insufficient and introduces additional security risks. Hackers are increasingly utilizing "SIM Swap Attacks" as a means to gain control over a victim's phone number and receive all the text messages and voice calls intended for the victim. After a successful SIM Swap, the victim's smartphone will lose connection to the network and text messages intended for the victim will get redirected to the hacker's smartphone, allowing the hacker to view the victim's Text Message 2FA Notifications. The hacker can now bypass security safeguards on the victim's email and exchange accounts that rely on Text Message 2FA.

Implementing the following best practices will defend against such attacks and keep a user's assets safe:

1. Avoid using a primary or publicly identifiable email address to access exchange accounts - Create a separate, secret email address that will only be utilized for an exchange account.
2. Utilize a 2FA App, such as Google Authenticator, for securing email and exchange accounts - **do NOT use text messages for 2FA**.
3. "Whitelist" withdrawal addresses on exchange accounts. By doing so, digital currency can only be transferred to pre-approved, whitelisted addresses. If an account is compromised the hacker can only send digital currency to the user's own address.
4. Remove the Inherent Risk - **"Not your Keys, Not your Coins!"** Users should always own their private keys and store their digital currency offline. Do NOT store digital currency on exchanges. Users should secure private keys with hardware devices, such as: Ledger Wallet.

SIM Swap Attacks – How Hackers do it
A SIM Swap occurs when a hacker gathers enough personal information about a victim to successfully impersonate them. This is achieved through social engineering or purchasing information about a victim from Cyber Criminals on the Black Market. The hacker will convince the victim's phone carrier to switch the victim's number over to a SIM Card on a smartphone the hacker controls. Phone Carriers are easily deceived because SIM Swapping (Phone Porting) is commonly requested when a customer has lost or is replacing their smartphone because it allows the customer to seamlessly access their phone number on their new device.

A successful SIM Swap Attack occurs when the victim's smartphone loses connection to the network and the hacker's smartphone now receives all text messages and calls intended for the victim. 2FA Text Message Security Notifications are now received by the hacker. With access to

the victim's 2FA, the hacker can now gain control of the victim's email accounts, reset their credentials, and ultimately steal the victim's digital currency. In 2019, one investor had over $24 million worth of Bitcoin stolen in a SIM swap attack. On February 22, 2020 another investor lost $45 million in BTC and BCH overnight via Sim Swap Attack. Luckily, there are steps digital currency users can take to protect themselves from this sort of attack.

How Hackers use SIM Swaps to Access Email and Exchange Accounts

1. The hacker identifies a victim as an attractive target after noticing the victim's excessive, obnoxious tweets making predictions on XRP and Dogecoin.
2. By examining the victim's online footprint, the hacker identifies the victim's phone number, email address and other personal information (people frequently post their email addresses and phone numbers on their social media profiles).
3. The hacker then calls the victim's phone carrier, impersonates the victim, claims that the phone is lost and convinces the phone carrier to port the victim's phone number to a SIM the hacker controls.
4. The hacker now controls the victim's phone number and receives any one-time pass code reset messages sent via text message.
5. The hacker will proceed to initiate the password reset process on the victim's primary email account.
6. The hacker then receives the 2FA verification code (text message) and proceeds to reset the victim's email account password. The hacker now controls the victim's smartphone AND primary email account.
7. Once the hacker controls the victim's smartphone and email account they can begin the password reset process on the victim's digital currency exchange accounts. By selecting "Forgot Password," a temporary password will get sent to the victim's primary email account.
8. After the hacker resets the victims exchange account password, they proceed to login and withdraw all of the victim's digital currency to a wallet address controlled by the hacker.

4 Best Practices for Keeping Your Digital Currency Safe

1. **Create a Separate, Secret Email Account for Accessing Exchanges**
   When creating an exchange account do not use your primary email address as your login name. Instead, create a separate, secret email address that will only be used for accessing the exchange and receiving exchange-related notifications. Do not share your exchange account email address with others and do not use it to interact with any online platforms. Be sure to secure all your accounts with a 2FA App.

2. **Two-Factor Authentication (2FA) Applications**
   Relying solely on your username, passwords and text message verification for 2FA on your email and digital currency exchange accounts is a point of failure. 2FA Apps like Google

Authenticator verify your identity through your specific device (rather than your phone number) and your accounts are therefore no longer susceptible to SIM Swap Attacks. First step is to download and install the Google Authenticator 2FA App on your smartphone. You can then use the app to secure your accounts that support this type of 2FA (such as Gmail and Coinbase). During the setup process, you will be prompted to write down a unique backup code that will allow you to generate your 2FA Account on a different device. This is critical in case you ever lose access to your smartphone. Be certain to write down and store your backup code in a secure location that you can access at a later date, if needed.

3. **Whitelisting Withdrawal Addresses**
   Most digital currency exchanges allow users to "whitelist" withdrawal addresses. This means that your account will only be able to make withdrawals to the addresses you whitelist in advance. Therefore, if your exchange account is ever compromised, the hacker can only send the digital currency to an address that you have previously verified (which you should be in control of). This is the final layer of security for your exchange account. Even if your account gets hacked, the only possible address your funds can be sent to is your offline ledger.

4. **Securing your Private Keys with Hardware Devices**
   Digital currency held on exchanges are honeypots for hackers. Storing your digital currency offline via hardware devices like Ledger Wallet's Nano S keeps your tokens safe. Always purchase your hardware wallets directly from the manufacturer. Never buy them from a reseller as the integrity of the device may have been compromised.

   When setting up your hardware wallet for the first time, you will be prompted to record a list of 24 words on a piece of paper. These words are your "backup phrase" in case you need to restore your wallet data on another device in the event your original device is damaged or lost. Make sure you store your backup phrase in a secure location that you can access at a later date, if needed. If a 3rd party gains access to your backup phrase, they will be able to access your wallet from another device and steal your digital currency.

   Before sending all your digital currency to your hardware wallet, test the device's recovery function to ensure that you can restore your wallet data with your unique 24-word backup phrase. To test that your hardware wallet's backup mechanism functions correctly, follow the steps below (the steps below are for a Ledger Nano S Hardware Wallet and may vary slightly depending on the type of hardware device you purchase):

   1. Send an insignificant amount of coin to an address secured by your ledger.
   2. Enter the wrong pin three times *or* go to "Settings" and click "Reset" and you will be prompted to set-up your Ledger as a new or existing device. Choose "existing device".
   3. You will then need to enter each of the 24 words. This is somewhat time consuming, but well worth it.

4. After correctly entering the first three letters of the word you have recorded, you will be presented with a selection of words, one of which will be the correct one.
5. After repeating this procedure and confirming you have all the words from number 1 to 24 entered correctly you will receive a message informing you that the device has successfully restored. If not, try again.
6. If you continue to get the "Backup Failed" message go to "Settings", click "Reset", and set-up the Ledger as a "new device". This will involve going through the whole procedure of recording a (new) set of 24 words. After doing this, go back to the first step and proceed through the bullet points until you have successfully restored your device using your backup phrase.
7. Once restored, assure the incremental amount of coin is still accessible through the ledger.[1]

Not your Keys, Not your Coins!

Bitcoin and most digital currencies are bearer instruments, which means whoever possesses the private key owns the assets. This comes with an important trade-off: for the first time ever, users are able to own bearer instruments that are digital. However, this now requires users to take more responsibility for the security of their own digital currency. A feature of Bitcoin is immutability. Immutability is also unforgiving towards mistakes. Therefore, it is imperative for users to understand how to properly secure their online accounts and private keys. **"Not your Keys, Not your Coins."**