4/6/2021

Protect Your Crypto (Warning Your Crypto Is Not Safe - Koroush AK)

- 12/15/2020 This week, the owner of Nexus Mutual was hacked for $8,000,000 through crypto. His name is Hugh Karp.
- Guy does technology for a living. If he can get hacked, anybody can according to Koroush AK.
- He went to use his metamask wallet and there was malware in his browser
  - The malware gave him a spoof approval for a transaction and he approved it. thus sending the $ into the hackers wallet.
- Blockchain and blockchain exchanges are not remotely related to banks in the sense that once you make a transaction, the transaction is made. No reversing.
- No 3rd party manages this, its all done through mathematics algorithms and coding.
- If you do get hacked you can call the relevant authorities
- They can track the money to the wallets and then freeze the wallet in some cases
- Cryptocurrency Security Guide
- Koroush AK partnered w/ NGRAVE who is "an innovative cryptocurrency security company" to create and support this article.
- Step 1: Defense Software
  - Download and run regularly scheduled scans
    - Antivirus (Bitdefender)
    - Antimalware (MalwareBytes)
    - Firewall (ZoneAlarm Pro Console)
- Step 2: VPN
  - Helps you do your work through a secure tunnel so hackers can't access data
  - Download turn on keep on
  - Ex: NordVPN

- Step 3: Cryptocurrency Storage
  - Essential. Wallets in Slut.
  - 3 Tiers (AK says no reason not to go Tier 1)
    1- Hardware Wallets
      - NGRAVE ZERO, protects from multiple attack vectors
        - Offline from secret key generation to transaction signing
        - Called the coldest wallet and easy to set up
        - AK's top choice but not too time tested as new company.
      - Trezor
        - The OG Hardware wallet, been around a long time and is time tested. Offers solid security
        - Difficult user interface (UI) apparently
    2- Paper Wallet
      - Stupid. Not even sure 100% how this works (like the other options too)
      - Use a pen/paper to Jot down your keys/passwords
      - Would need a safe or somewhat
    3- Desktop Wallet
      - Also stupid
      - Only as safe as the system they're on.
      - Ex. Exodus or Metamask (guy got hacked $8M on metamask)
- Step 4: 2 Factor Authentication (2FA)
  - You can use your phone and enable text msgs as an authentication
    - DON'T DO THIS. Sim swappers can hack and verify.
  - COLD 2FA devices are essential
    - ZERO will double up your FA (Tier 1)
    - YubiKey is a cold 2FA device as well (Tier 2)
    - Authenticator Apps on tablet or phone never connect that phone to internet again. SOLO authentication device really.

4/6/2021

Protect Your Crypto continued

- Step 5: Seperate Computers
  - At your discretion. AK uses 2 b/c he's loaded of course.
  - ~~Can opt for high security computers~~ High security comp is used only for crypto, banking, trading, and other crucially sensitive activities. Do not use Windows. Use a Mac, Linux, or ChromeOS
  - Low security computer takes care of everything else. Never switch these up.
- Step 6: Password and Data Storage
  - This limits the damage a hacker can do
  - AK's Multilevel System
    - Level 1 Data
      - The type info that if a hacker has, they can attack you in some way
      - Your keys, SSN, passwords, recovery phrases, etc.
      - To be kept offline, never stored on a laptop ~~or~~ even for a second.
      - When entering the passwords, you will enter it in alternating between your on screen keyboard and your actual keyboard.
        - Requires the hacker to both have ~~B~~ your key logged and be able to see your screen to see your password
          - These passwords should be a min of 15 keys long and as complex as possible.

- Options to Store Your Level 1 Data
  - Storage (Tier 1)
    - Aforementioned ZERO will function as a password manager
    - GRAPHENE
      - A cryptographic puzzle made of 2 fire, water, buried and shockproof everlasting stainless steel plates.
      - Backs up your private keys / passwords if you set it as your manager
      - Recoverable protection against anything happening to your ZERO
  - Level 2 Data
    - Any data which on its own it can't be obtained and used for attack against you.
    - Should still be randomly generated by your password manager
- Step 7: Emails
  - Old emails w/ lackluster passwords = common entry pt for hackers
  - Get rid of old emails.
  - Master emails
    - To be made using Protonmail
      - Used for exchanges, banking, investing, etc
      - Also used for backing up Secondary emails.
  - Secondary Emails
    - At your convenience.
    - All emails should have 2FA.

4/6/2021

Protect Your Crypto Continued

- Step 8: Exchanges
  - Risky to use. Hackers lurk.
  - Only use reputable exchanges
  - Only use exchanges on your high security device.
  - Must be backed by master email, cold device device 2FA, and a secure password
  - Set a global lock that requires a min. wait time before settings are changed
    - If no plans/need to w/draw funds in the short term, set a large min wait time.
  - Use leverage as a means of reducing counterparty risk
    - Read/Watch AK tutorial abt doing so.
  - Whitelist your addresses and set a lock on adding new addresses.
- Step 9: Protect Your Friends/Family
  - If a hacker gets sensitive info abt friends/fam. they can leverage that to blackmail you.
  - Share these tips w/ them.