Risks & Mitigation

All Potential Crypto Risks

Clipboard Manipulator

- **RIsk**: A virus could view your clipboard and if it detects a wallet address, it could change it with an attackers address
- **Mitigation**: Check first and last 8 digits of address

Loosing Hardware wallet

- **Risk**: Someone could find the hardware wallet and try to brute force the pin
- **Mitigation**: Keep in a secure location

Loosing seed phrase

- **Risk**: Someone could find the seed phrase and drain the wallet
- **Mitigation**: Store 2 copies in 2 locations, on metal and paper

Sending to wrong address

- **Risk**: Send stuff to wrong address and it's lost forever :(
- **Mitigation**: Send small test transaction first then for large sends, verify FULL address

Website DNS attack

- **Risk**: An attacker could hijack a website DNS to point it to a different location (domain is still the same but code is different)
- **Mitigation 1**: Set up a second wallet for ongoing transactions when interacting with sites and not ledger software
- **Mitigation 2**: Check website's twitter page for any announcements

Protocol code / private key attack

- **Risk**: A protocol's private keys or code gets hacked
- **Mitigation**: Don't hold too much % in a defi project / memecoin

CEX closes / limits account

- **Risk**: Exchange closes / limits account
- **Mitigation**: Sign up to multiple exchanges\

Cookie Stealer

- **Risk**: Install a virus that steals all session cookies and can now log into any website already logged into
- **Mitigation**: Don't install software you don't 100% trust OR have a seperate computer / OS for crypto transactions

Bank blocks deposit

- **Risk**: Bank blocks a deposit from your account to a crypto exchange
- **Mitigation 1**: Sign up to multiple bank
- **Mitigation 2**: Buy the bitcoin ETF

Phishing

- **Risk**: Someone sends an email / text / call pretenting to be an exchange or wallet
- **Mitigation**: Check sender from address, go directly to URL, don't click link, ensure 2FA is enabled on exchanges

Sim Swap attack

- **Risk**: Someone finds out my phone number and sends my number to their phone to try and reset password linked to my phone
- **Mitigation**: Ensure app based codes are enabled over phone number based

Best Mitigation Techniques

In order of Hardest to easiest

1. Have a seperate computer for crypto transactions (preperably with linux)
2. Have a seperate browser profile with only ublock origin
3. Check full address for big transactions
4. Send a test transaction for new addresses

Revision #1
Created 22 March 2025 10:02:45 by Conor
Updated 22 March 2025 10:03:47 by Conor