Wallet Audit Client 1

SovereignTzu

January 20, 2024

Contents

1 About **1**

2 Disclaimer **1**

3 Introduction to the Audit Methodology **2**

3.1 Attack Vectors Assessed . . . 2

3.2 Scoring System . . . 2

4 About Client **2**

5 Risk classification - The risk classification table **2**

5.1 Impact . . . 3

5.2 Likelihood . . . 3

5.3 Action Required for Severity Levels . . . 3

6 Executive Summary **3**

6.1 Finding Count . . . 3

6.2 Summary of Findings . . . 3

7 Findings **3**

7.1 (H-01): Open Smart Contract Approvals . . . 3

7.2 (M-01): Lack of Antivirus . . . 4

7.3 (M-2): 2FA with Phone Number . . . 4

7.4 (M-3): Seed Phrase Storage . . . 4

7.5 (L-01): Ghost Wallet Change . . . 4

7.6 (IN-01) Future proof cold wallet need . . . 4

7.7 (IN-02): Regular software updates . . . 5

8 Wallet Audit Score **5**

8.1 Audit Score Count . . . 5

8.2 Post Audit Score . . . 5

1 About

Sovereign Wallet Guard is a boutique consulting firm committed to enhancing your cryptocurrency security. Our mission is to provide personalized advice, tailored to your individual needs. In a market saturated with generic security tools and products, many of which offer a false sense of safety, we stand out by focusing on practical, applicable solutions. We believe the best security tips are those you can realistically implement.

2 Disclaimer

While Sovereign Wallet Guard strives to enhance your crypto wallet's security, no audit can guarantee complete immunity from vulnerabilities. Our recommendations aim to significantly mitigate risks, potentially reducing losses from threat actors. However, the final responsibility for wallet security rests with you as the owner.

3 Introduction to the Audit Methodology

In our Sovereign Wallet Security Audit, we employ a meticulous methodology focused on evaluating a comprehensive set of potential attack vectors that could impact the security of your cryptocurrency wallet. This methodology is designed to systematically assess each critical aspect of your wallet's security and provide you with a clear, quantifiable understanding of your current security posture.

3.1 Attack Vectors Assessed

1. VPN Usage
2. Antivirus Protection
3. Cold Wallet Security
4. Hot Wallet Hygiene
5. Two-Factor Authentication (2FA)
6. Seed Phrase Security
7. Password Strength
8. Offline Security Practices
9. Social Media Exposure
10. Airdrop Participation Risks
11. Browser Security
12. Transaction Security
13. Smart Contract Approvals
14. Wallet Connections

3.2 Scoring System

We apply a scoring system with three possible scores in each category:

- 0 (Poor): Indicates significant vulnerability or a lack of protective measures.
- 0.5 (Moderate): Shows partial security measures in place, but with room for improvement.
- 1 (Good): Reflects robust security practices and a high level of protection.

4 About Client

The client is an active investor in large-cap cryptocurrencies, focusing on stable, high-market-cap assets. In addition to traditional crypto investments, they are engaged in staking activities, contributing to blockchain network operations and earning rewards.

5 Risk classification - The risk classification table

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

5.1 Impact

- High Impact: This leads to a significant loss of assets in the wallet. This level of impact requires immediate attention.
- Medium Impact: This may lead to a small loss of funds. It's serious but not as immediately threatening as high impact.
- Low Impact: This could result in unexpected behavior affecting wallet functionality, but it is not critical to asset security.

5.2 Likelihood

- High Likelihood: Common attack vectors such as phishing through social media, insecure handling of seed keys, and exposure on platforms like Discord and Twitter.
- Medium Likelihood: More sophisticated attacks like supply chain attacks, or risks associated with digital copies of seed phrases.
- Low Likelihood: Rare scenarios such as corrupt hardware or extremely sophisticated digital breaches

5.3 Action Required for Severity Levels

- Critical: Immediate action required. Failure to address this may result in a significant and immediate risk to assets.
- High: Should be resolved promptly to prevent potential loss.
- Medium: Advised to fix. Often related to 'features, not bugs' that could become exploitable.
- Low: Generally 'features not bugs'. Low priority but should be monitored for changes in the threat landscape.

6 Executive Summary

6.1 Finding Count

Severity	Amount
High	1
Medium	3
Low	1
Informal	2
Total Findings	7

6.2 Summary of Findings

ID	Title	Severity	Status
(H-01)	Open Smart Contract Approvals	High	Pending
(M-01)	Lack of Antivirus	Medium	Pending
(M-02)	2FA with Phone Number	Medium	Pending
(M-03)	Seed Phrase Storage	Medium	Pending
(L-01)	Ghost Wallet Change	Low	Pending
(IN-01)	Invest in a cold wallet for future use	Informal	Pending
(IN-02)	Regular software updates	Informal	Pending

7 Findings

7.1 (H-01): Open Smart Contract Approvals

- Severity: High
- Impact: High, as this can lead to total loss of funds.

- Likelihood: Medium, since there have been multiple smart contract protocols that have been exploited. This has led to open approvals holders being exploited.
- Description: To interact with smart contract protocols, a user has to allow the protocol to spend tokens on their behalf. By default, the spending limit is left unlimited. If these unlimited approvals are not revoked, the funds' safety depends on the protocol's safety.
- Recommendation: Use a tool such as revoke.cash or Wallet Guard to revoke approvals. Another solution is to always transfer funds to a software wallet that does not interact with any protocols/websites.

7.2 (M-01): Lack of Antivirus

- Severity: Medium
- Impact: High, leaves your computer vulnerable to malware
- Likelihood: Low, but has a high impact if it occurs
- Recommendation: Purchase an antivirus of your liking. If you're using a Windows computer, Windows Defender is sufficient. For Mac, Malwarebytes is a good choice.

7.3 (M-2): 2FA with Phone Number

- Severity: Medium
- Impact: High, having 2FA with phone number leaves you vulnerable to SIM swapping. This will lead to loss of access to social media accounts, CEX exchange accounts, etc.
- Likelihood: Low, since you have to be a high-value target to be compromised.
- Recommendation: If possible remove 2FA with the phone number and replace it with 2FA connected to an authentication app or a Yubikey.

7.4 (M-3): Seed Phrase Storage

- Severity: Medium
- Impact: High, if compromised will lead to loss of potentially all funds.
- Likelihood: Low, since this is a highly targeted effort.
- Description: Storing seed phrases digitally is not recommended because of the risk of seed phrases being leaked/compromised.
- Recommendation: Have multiple online paper-backed versions of the seed phrase.

7.5 (L-01): Ghost Wallet Change

- Severity: Low
- Impact: Medium, using the same ghost wallet for a long period increases the risk of the ghost wallet being compromised/targeted by threat actors.
- Recommendation: It's a good routine to change the wallet that is used to interact with protocols/connected with sites. It's free and mitigates the risk of interacting with scam tokens.

7.6 (IN-01) Future proof cold wallet need

- Proactively planning for the eventual need of a cold storage wallet is a prudent step. It's advisable to acquire a hardware wallet in advance to ensure it's ready when needed. Companies like Ledger or Trezor are reputable sources for purchasing hardware wallets. These devices are essential for enhanced security of your assets, especially as your portfolio grows. To avoid risks of tampering, always purchase hardware wallets directly from the manufacturers or their authorized dealers. Avoid resellers, as the integrity of the device cannot be guaranteed.

7.7 (IN-02): Regular software updates

- It is crucial to regularly update your software wallet. Updates often include patches for security vulnerabilities, both known and newly discovered, ensuring enhanced protection against potential threats.

8 Wallet Audit Score

8.1 Audit Score Count

After assessing all the 14 attack Vectors this was the Score count

Attack Vector	Score
VPN Usage	1
Antivirus Protection	0
Cold Wallet Security	0.5
Hot Wallet Hygiene	1
Two-Factor Authentication (2FA)	0.5
Seed Phrase Security	0.5
Password Strength	1
Offline Security Practices	1
Social Media Exposure	1
Airdrop Participation Risks	1
Browser Security	1
Transaction Security	1
Contract Approvals	0
Wallet Connections	0
Total Score	9.5/14

8.2 Post Audit Score