Wallet Audit Client 2

SovereignTzu

January 28, 2024

Contents

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

Our client is an OG diamond hand Ethereum holder. This long-term holding strategy underscores their early belief in Ethereum's potential. The primary focus of our audit is to ensure the enduring security and modernization of their digital asset storage.

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.
- Informal: Low priority, good to know and should monitor for changes in the threat landscape.

6 Executive Summary

6.1 Finding Count

Severity	Amount
Critical	1
High	2
Medium	2
Informal	1
Total Findings	6

6.2 Summary of Findings

ID	Title	Severity	Status
(C-01)	Self-Custody of Funds	Critical	Pending
(H-01)	Transaction Hygiene	High	Pending
(H-02)	Airdrop Exposure	High	Pending
(M-01)	Lack of Antivirus	Medium	Pending
(M-02)	2FA with Phone Number	Medium	Pending
(IN-01)	Regular software updates	Informal	Pending

7 Findings

7.1 (C-01) Self-Custody of Funds

- Severity: High
- Likelihood: High

- Description: With the current arrangement of not holding personal funds independently. The funds are currently managed via a software wallet on an older desktop. While this setup offers robust security for long-term holding due to limited accessibility, it also presents a significant downside. The primary concern here is the lack of personal control and hands-on experience in managing digital assets, which is crucial for active participation in the crypto space.
- Recommendation: * Transition to Self-Custody: To gain better control and security over your funds, we recommend transitioning to a hardware wallet, specifically a Trezor model. This change will empower you with direct management of your digital assets while offering enhanced security. If you prefer to continue with a trusted individual managing your funds, this is acceptable. However, we recommend staying informed about your wallet's status and transactions.

7.2 (H-01): Transaction Hygiene

- Severity: High
- Likelihood: High
- Description: Keeping your transactions clean is crucial for ensuring your funds end up where they're supposed to. A small mistake in the address or choosing the wrong network can result in lost funds. Additionally, there's a sneaky trick called address poisoning, where scammers watch for transactions and then send funds from a lookalike address, hoping you'll use it for your next transaction by mistake.
- Recommendation: Always double-check the address you're sending to, and make sure you're on the correct network for the transaction. This is like confirming the ZIP code on a package, make sure it arrives. Before making a transaction, verify the address with the recipient through a separate channel if possible. Be alert for address poisoning: if you receive funds from an unknown source that looks similar to a known address, proceed with caution. It's a good idea to use address book features in wallets to save and label addresses you trust, minimizing the risk of errors or falling for scams.

7.3 (H-02): Airdrop Exposure

- Severity: High
- Likelihood: High
- Description: Since the funds have been held for such a long time, your wallet is eligible for valuable airdrops. These airdrops, are valuable but can put you at risk of losing all your funds if not setting up the correct infrastructure to participate safely. Some airdrops might require interacting with new contracts or platforms, which could expose you to vulnerabilities or scams.
- Recommendation: Before you get involved in any airdrop, it's crucial to set up a separate wallet specifically for these events. This way, your main holdings stay safe, even if something goes wrong. Always do thorough research on any airdrop you're considering. Look into the project's background, the team, and community feedback. Never share your private keys or send any of your own funds to participate in an airdrop. If an offer sounds too good to be true, it probably is. Using a separate wallet for airdrops not only minimizes your risk but also keeps your primary wallet's transactions and balances private.

7.4 (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 Premium is a good choice.

7.5 (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 must be a high-value target to be compromised.
- Recommendation: Replace 2FA with the phone number and replace it with 2FA connected to an authentication app or a Yubikey.

7.6 (IN-01): 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	0.5
Cold Wallet Security	0.5
Hot Wallet Hygiene	0.5
Two-Factor Authentication (2FA)	0
Seed Phrase Security	0
Password Strength	0.5
Offline Security Practices	1
Social Media Exposure	1
Airdrop Participation Risks	1
Browser Security	1
Transaction Security	0
Contract Approvals	0.5
Wallet Connections	0.5
Total Score	7/14

8.2 Post Audit Score

9 Recommendations for Mitigation and Improvement

9.1 Transition to Self-Custody

To gain better control and security over your funds, we recommend transitioning to a hardware wallet, specifically a Trezor model. This change will empower you with direct management of your digital assets while offering enhanced security.If you prefer to continue with a trusted individual managing your funds, this is acceptable. However, we recommend staying informed about your wallet's status and transactions.

9.2 Enhance Transaction Security

Educate yourself on proper transaction protocols, such as double-checking recipient addresses before confirming transactions. Learn to discover address poisoning etc.

9.3 Smart Contract Interaction

Use tools like, revoke.cash, and Wallet Guard to manage and review smart contract approvals effectively. This will help in avoiding unauthorized access to your funds.

9.4 Password Management

Implement a robust password management system, either through an external manager or your browser's built-in feature, to secure your digital accounts.

9.5 Two-Factor Authentication (2FA)

At the very least, set up app-based 2FA (Google authentication app or MicroSoft authentication app) for an additional security layer. For even greater security, consider using a YubiKey.

9.6 Email Management

Maintain separate email accounts for cryptocurrency exchanges and your personal online transactions to enhance security and organization.

10 End note

By addressing these areas, you can significantly improve the security of your crypto assets and gain a more comprehensive understanding of the crypto ecosystem.