satwise

SEED PHRASE BEST PRACTICES AND SECURITY

ABSTRACT

Best practices for Bitcoin seed phrase protection, management and security

Zach Peters
Bitcoin Security

Seed Phrase Best Practices

The BIP-39 seed phrase is a set of 12 or 24 words that serves as the master key to your Bitcoin wallet, including devices like the COLDCARD Mk4. It deterministically generates all private keys for your wallet, making it the single most critical piece of information for accessing your funds. Losing it means losing access to your Bitcoin, and if someone else obtains it, they can steal your funds instantly. Below, I explain the risks of AI searching for BIP-39 seed phrases and why you should avoid taking pictures or storing them digitally.

AI Searching for BIP-39 Seed Phrases

What It Is

AI-driven attacks involve using machine learning or computational algorithms to guess or brute-force a BIP-39 seed phrase. Since BIP-39 uses a fixed wordlist of 2048 words, the total possible combinations are finite but astronomically large:

- **12-word seed**: ~2^128 combinations (340 undecillion, or 340 followed by 36 zeros).
- **24-word seed**: ~2^256 combinations (even larger).

AI could theoretically be trained to narrow down this space by leveraging patterns, user behavior, or leaked data (e.g., partial phrases, common word combinations, or predictable entropy).

How AI Could Be Used

1 **Pattern Recognition**:

- AI models, like large language models or neural networks, can analyze leaked data (e.g., from hacks, phishing sites, or cloud breaches) to identify common seed phrase patterns or user tendencies (e.g., using memorable words or phrases).
- If users write weak passphrases or reuse patterns, AI could prioritize likely combinations.

2 **Social Engineering Analysis**:

- AI could scrape social media, emails, or public posts to infer user-specific details (e.g., birthdays, names, or hobbies) that might influence seed phrase choices if users deviate from random generation.

3 **Brute-Force Optimization**:

- While brute-forcing a full BIP-39 seed is infeasible (it would take billions of years even with supercomputers), AI could optimize guesses if partial information is known (e.g., a few words leaked via a photo or text file).
- Tools like BTCRecover use AI-driven techniques to recover wallets from partial or corrupted seeds, showing how such methods could be weaponized by attackers.

4 **Exploiting Digital Footprints**:

- If a seed phrase is stored digitally (e.g., in a photo, cloud drive, or text file), AI-powered malware or hacking tools could scan devices, cloud services, or even camera rolls to extract it.
- Modern AI image recognition (e.g., OCR) can easily read handwritten or typed seed phrases from photos, even if partially obscured.

Current Feasibility

- **Direct Brute-Forcing**: Practically impossible due to the massive keyspace (2^128 or 2^256). Even quantum computers (as of 2025) can't break this in a reasonable timeframe.
- **Targeted Attacks**: The real risk comes from partial leaks or poor security practices. AI excels at exploiting small bits of information (e.g., a few seed words, a predictable passphrase, or metadata from a photo).
- **Future Risks**: As AI and computing power improve, attacks could become more sophisticated, especially if users store seeds insecurely or use weak entropy.

Why You Should Not Take Pictures or Save Digitally

Storing your BIP-39 seed phrase digitally—whether as a photo, text file, email, or cloud backup—creates significant vulnerabilities. Here’s why you should avoid it:

1 **Device Compromise**:

- **Malware**: Phones, computers, or cameras can be infected with malware that scans for text files, images, or clipboard data containing

- seed phrases. AI-powered malware can use OCR to extract words from photos or screenshots.
- **Remote Access**: Hackers gaining remote access to your device (via phishing, exploits, or weak passwords) can access stored files or camera rolls.

2 **Cloud Syncing**:

- Many devices automatically back up photos or files to cloud services (e.g., iCloud, Google Photos, Dropbox). These services are frequent targets for hackers, and a leaked seed phrase could be extracted by AI tools scanning cloud data.
- Even if you disable auto-sync, metadata (e.g., EXIF data in photos) could reveal sensitive information like location or timestamp, aiding social engineering.

3 **AI-Powered Image Recognition**:

- Modern AI can read handwritten or typed text in images with high accuracy. A photo of your seed phrase (e.g., written on paper or displayed on a screen) could be processed by malicious software if your device or cloud is compromised.
- Example: A hacker accessing your Google Photos could run an OCR tool to extract "apple banana cherry" from a blurry handwritten note.

4 **Physical Exposure**:

- Taking a photo often involves displaying the seed phrase in an insecure environment (e.g., on a screen or paper in public). Someone nearby could capture it, or a security camera could record it.
- Photos stored on devices are often accessible to apps with camera roll permissions, increasing exposure.

5 **No Recovery Control**:

- Once a digital copy exists, you can’t guarantee it’s fully deleted. Even “deleted” files can be recovered from devices or cloud services unless securely wiped (e.g., using multiple overwrites or encryption).
- Cloud providers may retain backups even after you delete files, leaving a latent risk.

6 **Human Error**:

- You might accidentally share a photo (e.g., via messaging apps, social media, or email).

- Saving a seed in a text file labeled “wallet_seed.txt” or similar makes it an easy target for automated searches by hackers or AI tools.

Best Practices for Seed Phrase Security

To protect your BIP-39 seed phrase and mitigate risks from AI-driven attacks or digital leaks:

1 **Store Offline Only**:

- Write the seed phrase on paper (use the COLDCARD recovery card) or engrave it on a durable medium like a metal plate (e.g., Billfodl or CryptoSteel).
- Store in a secure location (e.g., fireproof safe, safety deposit box) with controlled access.
- Create multiple backups and store them in separate, secure locations (e.g., home and a trusted relative’s safe).

2 **Never Store Digitally**:

- Avoid taking photos, screenshots, or saving the seed in text files, emails, or cloud services.
- If you must type it temporarily (e.g., for import), use an air-gapped computer, delete immediately, and securely wipe the device.

3 **Use Physical Security**:

- Perform setup in a private, camera-free environment to avoid accidental exposure.
- Inspect storage locations for tampering regularly.

4 **Add a Passphrase**:

- Use a BIP-39 passphrase (a “25th word”) to add an extra layer of security. Memorize it or store it separately from the seed phrase. Even if the 12/24 words are compromised, the passphrase protects your funds.
- Example: Seed phrase + passphrase = unique wallet derivation.

5 **Test Recovery**:

- Periodically test your seed phrase on a testnet wallet or new device to ensure accuracy without risking real funds.
- Verify backups are legible and durable.

6 **Use COLDCARD Security Features**:

- Enable a duress PIN to access a decoy wallet in case of coercion.

- Use the COLDCARD’s tamper-evident bag and verify the bag number to ensure no physical compromise.
- Regularly check for firmware updates (verify signatures) to patch vulnerabilities.

7 **Avoid Predictable Patterns**:

- Always use the COLDCARD’s random seed generation—never create a “brain wallet” with predictable phrases (e.g., song lyrics or personal info), as AI could exploit these.

Why This Matters

The combination of AI’s ability to process vast datasets and the permanence of digital storage makes any digital copy of your seed phrase a ticking time bomb. A single breach—whether through malware, cloud hacks, or accidental sharing—could expose your seed to AI-driven extraction tools, leading to instant loss of funds. By keeping your seed phrase strictly offline and using secure practices, you eliminate the primary vectors for such attacks.

If you’re using a COLDCARD Mk4, its air-gapped design (via MicroSD) and tamper-resistant features are built to complement these practices. Stick to physical backups, verify everything, and treat your seed phrase like the key to your financial sovereignty—it is. If you have specific concerns about your setup or need help with a related task, let me know!